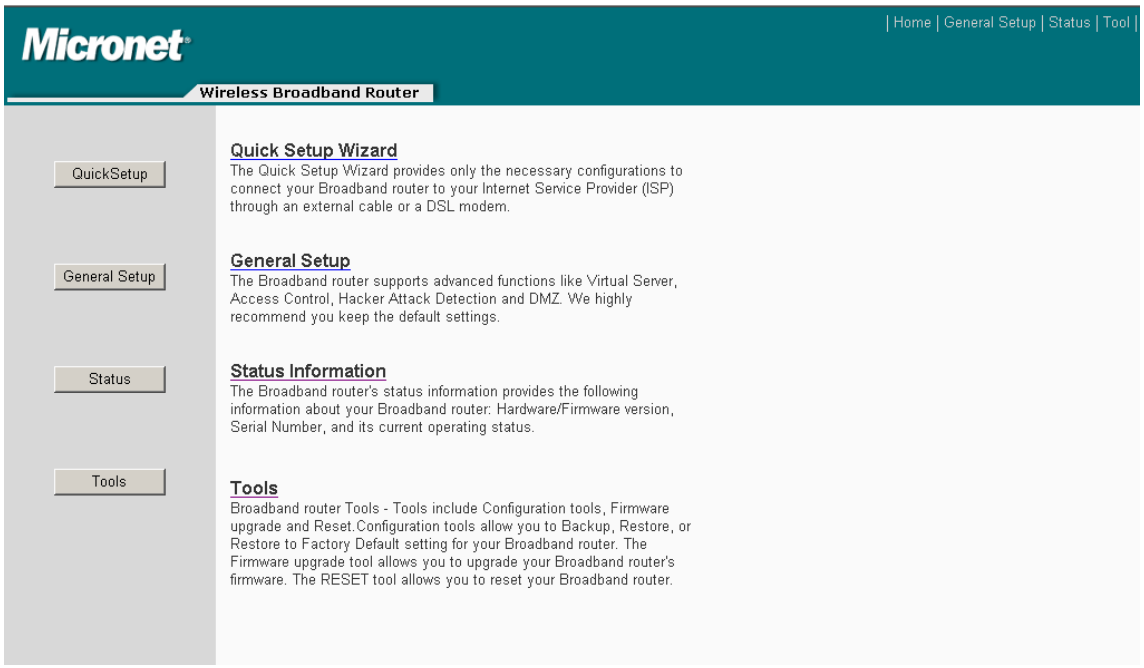
Micronet®
Faster and Easier Networks

Configuración Avanzada (Para Expertos)

4.2 Configuración general

En este capítulo, usted sabrá cómo cambiar la zona horaria, contraseña y las configuraciones de administración remota. Por favor, active el navegador de Internet y regístrese en la interfaz de administración Web del router, luego haga clic en el botón 'General Setup' a la izquierda o en el link 'General Setup' en el margen superior derecho de la interfaz de administración Web.


Micronet
Wireless Broadband Router
| Home | General Setup | Status | Tool |
QuickSetup
General Setup
Status
Tools
Quick Setup Wizard
The Quick Setup Wizard provides only the necessary configurations to connect your Broadband router to your Internet Service Provider (ISP) through an external cable or a DSL modem.
General Setup
The Broadband router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ. We highly recommend you keep the default settings.
Status Information
The Broadband router's status information provides the following information about your Broadband router: Hardware/Firmware version, Serial Number, and its current operating status.
Tools
Broadband router Tools - Tools include Configuration tools, Firmware upgrade and Reset.Configuration tools allow you to Backup, Restore, or Restore to Factory Default setting for your Broadband router. The Firmware upgrade tool allows you to upgrade your Broadband router's firmware. The RESET tool allows you to reset your Broadband router.

4.2.1 Sistema

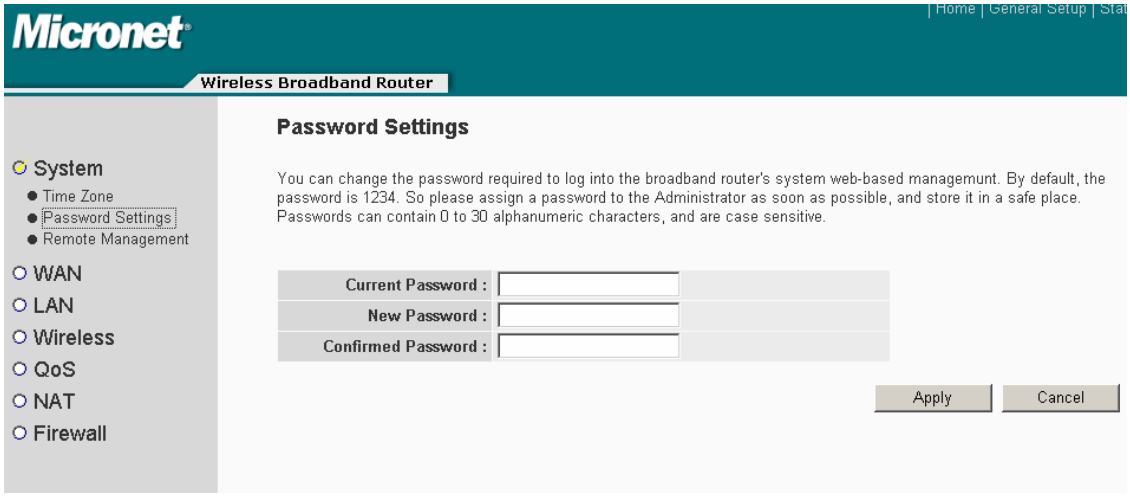
Esta sección le permite al usuario fijar la siguiente configuración del sistema: zona horaria, contraseña y el Administrador de Administración Remota.

4.2.1.1 Zona horaria y sincronización horaria automática

Por favor, haga clic en el menú 'System' a la izquierda de la interfaz de administración Web, luego haga clic en 'Time Zone' y el siguiente mensaje aparecerá en el navegador de Internet: *Please, select time zone at 'Set time zone' drop-down list, and input the IP address or host name of time server* (Por favor, seleccione la zona horaria en el menú desplegable 'Set time zone' e ingrese la dirección IP o el host name del servidor horario). Si usted desea activar la configuración de horario de verano, por favor marque la casilla 'Enable Function' y fije la duración de la configuración de verano.

4.2.1.2 Configuración de contraseña

La contraseña por defecto de fábrica de este router es ‘1234’ y aparece en la casilla para registrarse cuando se accede por un navegador de Internet. Existe un riesgo de seguridad si usted no cambia esta contraseña, ya que todos la pueden ver. Esto es muy importante cuando se inicia la función inalámbrica. Por favor, haga clic en el menú ‘System’ a la izquierda de la interfaz de administración Web y luego haga clic en ‘Password Settings’. Aparecerá el siguiente mensaje en su navegador de Internet.

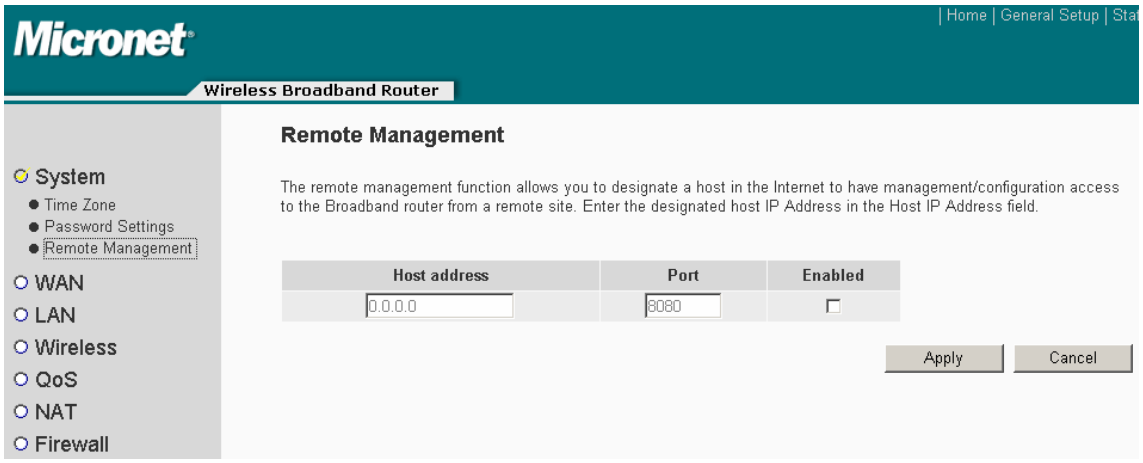

Micronet
Wireless Broadband Router
| Home | General Setup | Sta
System
Time Zone
Password Settings
Remote Management
WAN
LAN
Wireless
QoS
NAT
Firewall
Password Settings
You can change the password required to log into the broadband router's system web-based managemunt. By default, the password is 1234. So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive.
Current Password :
New Password :
Confirmed Password :
Apply
Cancel

Parámetro	Descripción
Current Password	Ingrese su contraseña actual para que el administrador de administración remota se conecte a su Broadband router. *Por defecto: sin contraseña.*
New Password	Ingrese la nueva contraseña.
Confirmed Password	Ingrese nuevamente la contraseña nueva para su verificación. Si se olvida la contraseña, tendrá que reiniciar el router a su estado inicial (sin contraseña) con el botón *reset* (ver panel posterior de router).

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.1.3 Administración remota

Este router no permite la administración de acceso desde Internet para evitar posibles problemas de seguridad (especialmente cuando los usuarios definieron una contraseña fácil o no cambiaron la contraseña por defecto). Sin embargo, los usuarios pueden administrar el router desde una dirección IP específica permitiendo la función ‘Remote Management’.

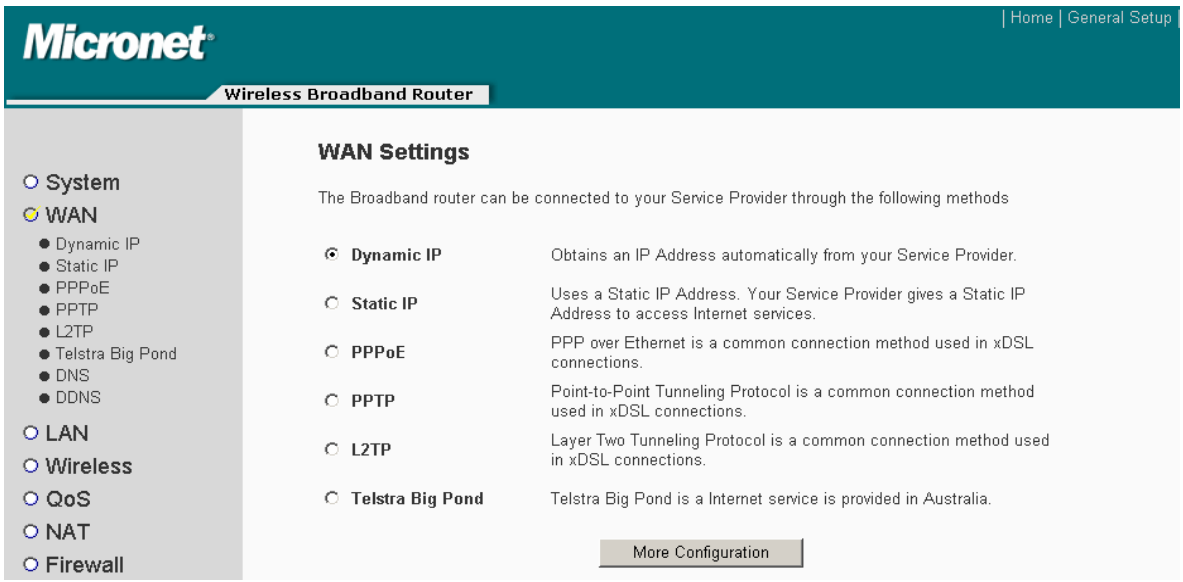


Parámetro	Descripción
Host Address	Ésta es la dirección IP del host en Internet que tendrá acceso a la administración/configuración del Broadband router desde un sitio remoto. Esto significa que si el usuario está en su casa y a la dirección IP de su casa se le ha asignado la dirección IP del host de la administración remota para este router (localizada en su oficina), entonces será posible configurar este router remotamente. Si la dirección de Host queda 0.0.0.0, significa que cualquiera puede acceder a la configuración del router basada en la Web desde una ubicación remota**,** si conocen la contraseña. Cuando el usuario quiere acceder a la administración Web desde un sitio remoto, es necesario ingresar la dirección IP WAN del router (ej. 10.0.0.1) en su navegador de Internet, seguida del número de puerto 8080 (ej. 10.0.0.1:8080). El usuario también debe saber la contraseña establecida en la pantalla Password Setting para acceder a la administración Web del router.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.2 WAN

La configuración de las conexiones a Internet se puede configurar usando el menú 'Quick Setup' descrito en el capítulo 4.1. Sin embargo, usted puede configurar las conexiones WAN usando el menú de configuración WAN. También puede configurar funciones avanzadas como DDNS (Dynamic DNS) a través de esta interfaz.


Micronet
Wireless Broadband Router
| Home | General Setup |
System
WAN
Dynamic IP
Static IP
PPPoE
PPTP
L2TP
Telstra Big Pond
DNS
DDNS
LAN
Wireless
QoS
NAT
Firewall
WAN Settings
The Broadband router can be connected to your Service Provider through the following methods
Dynamic IP
Obtains an IP Address automatically from your Service Provider.
Static IP
Uses a Static IP Address. Your Service Provider gives a Static IP Address to access Internet services.
PPPoE
PPP over Ethernet is a common connection method used in xDSL connections.
PPTP
Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.
L2TP
Layer Two Tunneling Protocol is a common connection method used in xDSL connections.
Telstra Big Pond
Telstra Big Pond is a Internet service is provided in Australia.
More Configuration

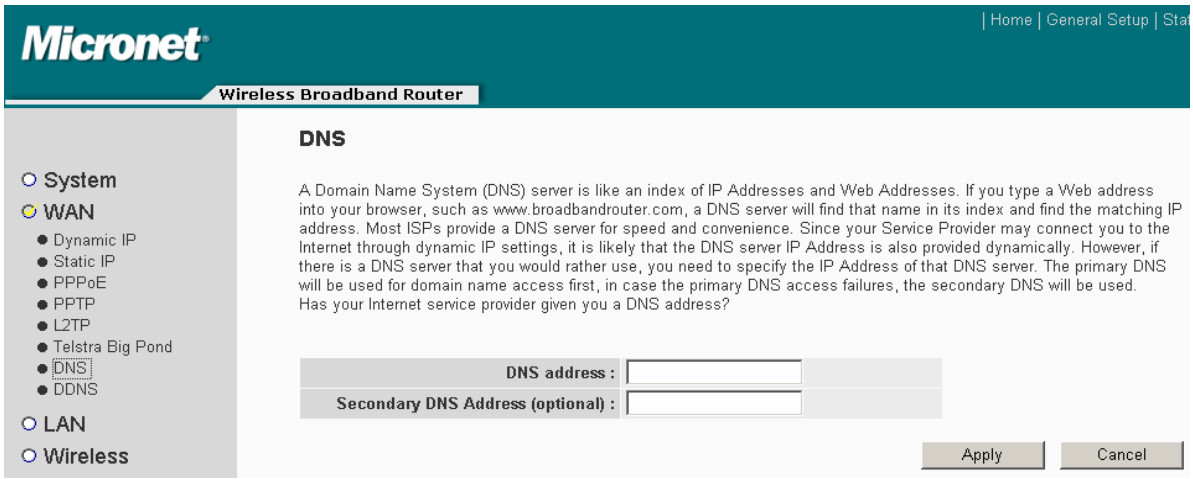
Parámetro	Descripción
Dynamic IP address	Su ISP le asignará automáticamente una dirección IP. Siga la sección 4.1 "Cable Modem" para más información.
Static IP address	Su ISP ya le ha asignado una dirección IP. Siga la sección 4.1 "Fixed IP" para más información.
PPPoE	Su ISP requiere usar una conexión Protocolo Punto a Punto sobre Ethernet (PPPoE) Siga la sección 4.1 "PPPoE" para más información.
PPTP	Su ISP requiere usar una conexión Protocolo de Túnel Punto a Punto (PPTP). Siga la sección 4.1 "PPTP" para más información.
L2TP	Su ISP requiere usar una conexión Protocolo de Túnel Capa 2 (L2TP).

Telstra Big Pond	Este Protocolo solo se usa para la conexión del ISP en Australia. Siga la sección 4.1 “Telstra Big Pond” para más información.
DNS	El usuario puede especificar un servidor DNS.
DDNS	El usuario puede especificar un servidor DDNS y configurar el nombre de usuario y contraseña proporcionadas por el proveedor de servidor DDNS.

*Haga clic en **<More Configuration>** al pie de la pantalla y prosiga hacia la subsección relevante del manual.*

4.2.2.1 DNS

Un servidor DNS (Domain Name System o Sistema de nombre de dominio) es como un índice de direcciones IP y direcciones de Web. Cuando un usuario ingresa una dirección de Web en su navegador, como por ejemplo www.router.com, un servidor DNS buscará ese nombre en su índice y la dirección IP que corresponda. La mayoría de los proveedores de servicios de Internet suministran un servidor DNS por una cuestión de velocidad y conveniencia. Si el proveedor de Internet conecta al usuario a Internet con una configuración IP dinámica, es probable que la dirección IP del servidor DNS se proporcione automáticamente. Sin embargo, si existe un servidor DNS que el usuario prefiera usar, es necesario especificar en esta sección la dirección IP de ese servidor DNS.

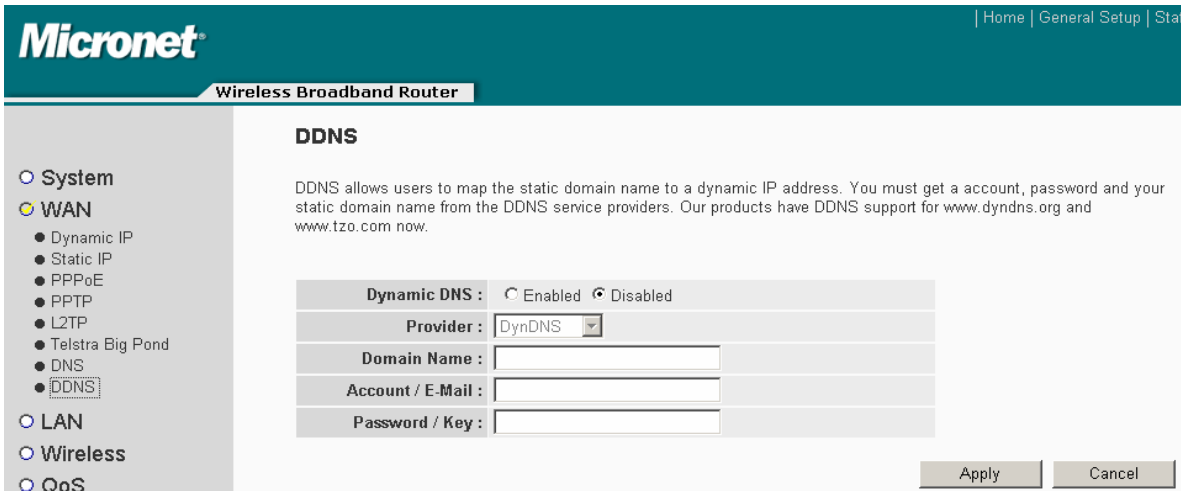

Micronet
Wireless Broadband Router
| Home | General Setup | Sta
System
WAN
Dynamic IP
Static IP
PPPoE
PPTP
L2TP
Telstra Big Pond
DNS
DDNS
LAN
Wireless
DNS
A Domain Name System (DNS) server is like an index of IP Addresses and Web Addresses. If you type a Web address into your browser, such as www.broadbandrouter.com, a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.
Has your Internet service provider given you a DNS address?
DNS address :
Secondary DNS Address (optional) :
Apply
Cancel

Parámetro	Descripción
Domain Name Server (DNS) Server	Ésta es la dirección IP del servidor DNS proporcionada por el ISP. El usuario puede especificar direcciones IP de servidores DNS de su preferencia.
Secondary DNS Address (optional)	Esto es opcional. El usuario puede ingresar una dirección IP de otro servidor DNS como backup. El DNS secundario será usado si el primero falla.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.2.2 DDNS

El DDNS permite al usuario mapear el nombre de dominio estático contra una dirección IP dinámica. El proveedor de servicios DDNS le debe suministrar al usuario una cuenta, una contraseña y el nombre de dominio estático. Este router admite DynDNS, TZO y otros proveedores comunes de servicios DDNS.



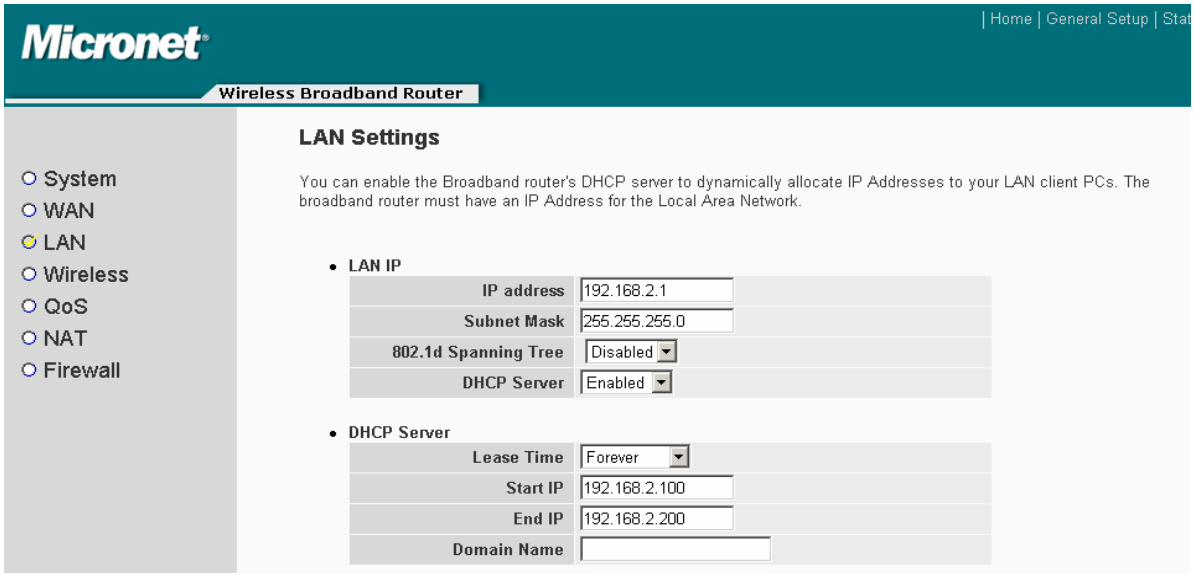
Parámetro	Descripción
Enable/Disable	Activar o desactivar la función DDNS de este router.
Provider	Seleccionar un proveedor de servicios DDNS.
Domain name	El nombre de dominio estático del usuario que usa DDNS.
Account/E-mail	La cuenta que el proveedor de servicios DDNS le asignó al usuario.
Password/Key	La contraseña configurada para la cuenta anterior de servicio DDNS.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.3 LAN

Antes de que todas las computadoras que usan conexión Ethernet por cable (es decir, esas computadoras se conectan al puerto LAN 1 a 4 de este router por cable Ethernet) se puedan comunicar entre ellas y acceder a Internet, deben tener una dirección IP válida. Existen dos maneras de asignar direcciones IP a las computadoras: dirección IP estática (la dirección IP se configura manualmente en cada computadora) y dirección IP dinámica (la

dirección IP de las computadoras se asignarán automáticamente por el router). Se recomienda para la mayoría de las computadoras el uso de dirección IP dinámica, ya que ahorrará una gran cantidad de tiempo en la configuración de direcciones IP. Las configuraciones DHCP solo están disponibles cuando 'DHCP Server' esté 'Enabled' en la sección 'LAN IP'.



Parámetro	Descripción
IP address	Ésta es la dirección IP del puerto LAN del router (dirección IP por defecto de la puerta de enlace de los clientes LAN).
IP Subnet Mask	Especificar una Máscara Subred para el segmento LANS.
802.1d Spanning Tree	Si la función 802.1d Spanning Tree está activada, este router usará el protocolo spanning tree para evitar bucles en la red en los puertos LAN.
DHCP Server	El usuario puede activar o desactivar el servidor DHCP. Al activar el servidor DHCP, el router les dará automáticamente a los clientes LAN una dirección IP. Si el DHCP no está activado, los usuarios tendrán que configurar las direcciones IP de los clientes LAN manualmente. Asegúrese de que el Cliente LAN esté en la misma subred que este broadband router para que el router sea la puerta de enlace por defecto del cliente LAN.
Lease Time	Cuando el DHCP esté activado les dará a los clientes LAN una dirección IP temporalmente. En la configuración Lease Time, los usuarios pueden especificar la cantidad de tiempo por la que el DHCP presta una dirección IP a los clientes LAN. El DHCP cambiará la dirección IP del cliente LAN cuando se llegue a este periodo umbral de tiempo.
IP Address Pool	Los usuarios pueden seleccionar un rango particular de dirección IP para que el servidor DHCP suministre direcciones IP a los Clientes LAN.

Domain Name	Los usuarios pueden especificar un Nombre de Dominio para la red LAN.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.3.1 Static DHCP Leases Table

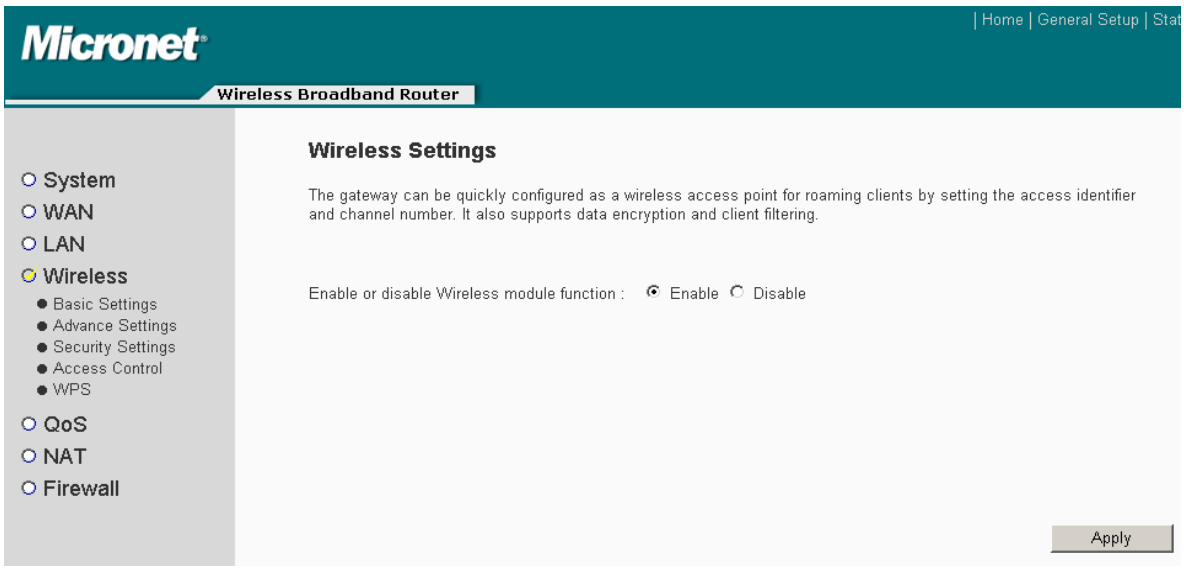
Esta función le permite asignar una dirección IP estática a una computadora específica para que no sea necesario configurar la dirección IP de una computadora y aun así poder disfrutar el beneficio de usar un servidor DHCP. Se puede asignar un máximo de 16 direcciones IP estáticas.

Parámetro	Descripción
Enable Static DHCP Leases	Tilde esta casilla para activar esta función.
MAC Address	Ingrese la dirección MAC de la computadora o dispositivo de red.
IP address	Ingrese la dirección IP para asignarle a esta computadora o dispositivo de red.

*Haga clic en **<Add>** para ingresar los datos en la tabla o **<Clear>** para borrar todos los caracteres.*

4.2.4 Inalámbrico

El Wireless Broadband Router construye una red inalámbrica LAN y permite que todas las computadoras equipadas con un adaptador de red inalámbrico IEEE 802.11b o 801.11g se conecten a Intranet e Internet. Admite encriptación WEP y WPA2 para mejorar la seguridad de la red inalámbrica.



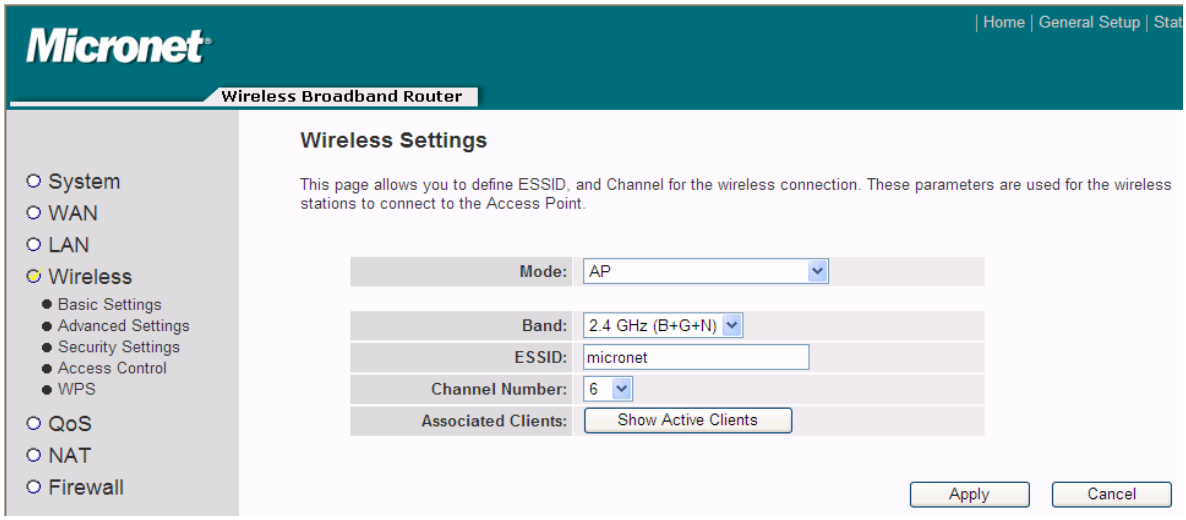
Parámetro	Descripción
Enable or Disable Wireless Module Function	El usuario puede seleccionar la activación o desactivación de la conexión inalámbrica de este dispositivo.

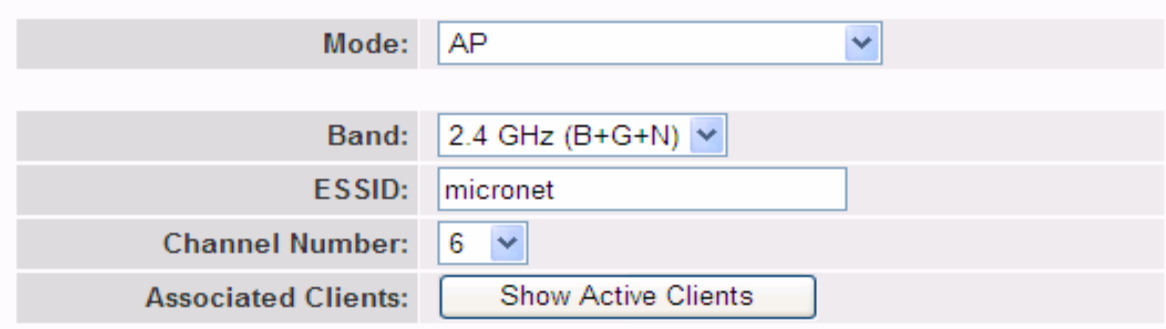
*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.4.1 Configuración inalámbrica básica

Por favor, haga clic en el menú 'Wireless' a la izquierda de la interfaz de administración Web, luego haga clic en 'Basic Settings' y aparecerá el siguiente mensaje en su navegador de Internet.

Modo: AP

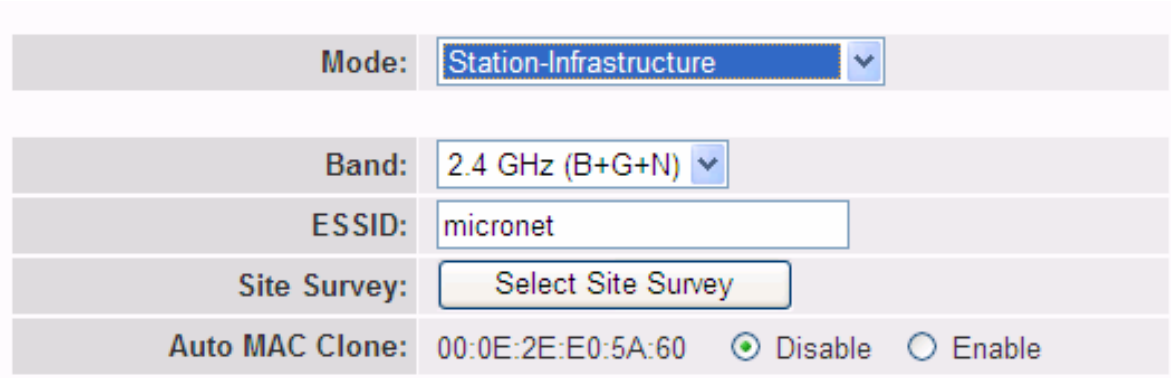




Parámetro	Descripción
Mode	Le permite al usuario configurar los siguientes modos: AP, Station, Bridge o WDS.
Band	Le permite al usuario configurar el modo AP para que quede fijo en 802.11b, 802.11g o 802.11n. Los usuarios también pueden seleccionar el modo B+G+N para que el router elija entre las conexiones 802.11b, 802.11g y 802.11n automáticamente.
ESSID	Éste es el nombre de la red inalámbrica LAN. Todos los dispositivos que estén en la misma red inalámbrica LAN deben tener el mismo ESSID.
Channel Number	El canal utilizado por la red inalámbrica LAN. Todos los dispositivos que estén en la misma red inalámbrica LAN deben utilizar el mismo canal.

Modo: Station – Infrastructure

En este modo, el usuario puede conectar el router a un dispositivo Ethernet como ser TV, consolas de juego, HDD&DVD para permitir que el dispositivo Ethernet sea una estación inalámbrica y se una a una red inalámbrica a través de un punto de acceso o router AP.

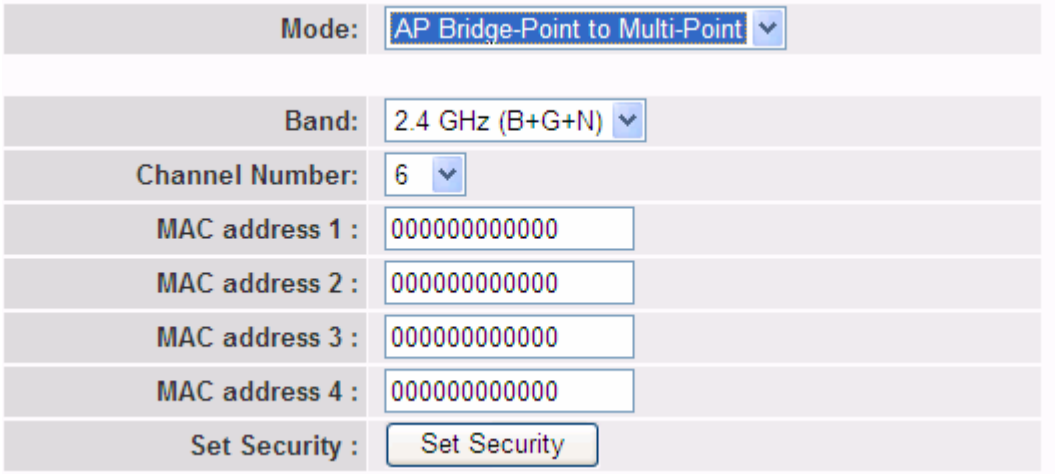


Parámetro	Descripción
Mode	Permite al usuario configurar el siguiente modo: AP, Station, Bridge o WDS.
Band	Permite al usuario fijar la configuración de AP en modo 802.11b, 802.11g o 802.11n. El usuario también puede seleccionar el modo B+G+N para permitir que el router seleccione entre las conexiones 802.11b, 802.11g y 802.11n automáticamente.
ESSID	Éste es el nombre de la red inalámbrica LAN. Todos los dispositivos de la misma LAN inalámbrica deberían tener el mismo ESSID.
Site Survey	Cuando el usuario utiliza este router inalámbrico como una estación inalámbrica para que el dispositivo de red Ethernet tenga capacidad inalámbrica, lo tiene que asociar a un punto de acceso activo. Haga clic en el botón 'Select Site Survey', y luego se abrirá la tabla "Wireless Site Survey Table". Aquí se enlistarán todos los puntos de acceso cercanos disponibles. El usuario puede seleccionar un punto de acceso de esta tabla y se unirá a la red inalámbrica LAN a través de este punto de acceso.
WLAN MAC	Para algunas aplicaciones, es posible que el usuario tenga que designar una dirección MAC específica para el router. Por favor, ingrese la dirección MAC aquí. Si usted está conectando el router a una computadora, simplemente puede presionar el botón 'Clone Mac address' para completar el campo de la dirección MAC con la dirección MAC de la computadora.

Modo: AP Bridge-Point to Point

En este modo, el usuario puede conectar su router inalámbrico al menos a cuatro routers inalámbricos para expandir el alcance de la red inalámbrica, y todos los clientes (solo los

que se conectan por cable; el modo AP no aceptará clientes inalámbricos en este modo) de los routers inalámbricos creerán que están en la misa red física.

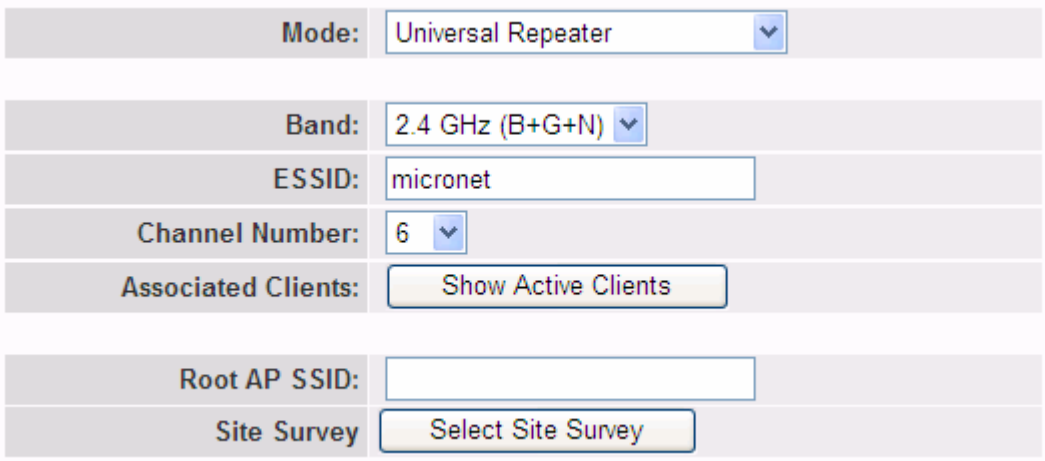


Parámetro	Descripción
Mode	Permite al usuario configurar el siguiente modo: AP, Station, Bridge o WDS.
Band	Permite al usuario fijar la configuración de AP en modo 802.11b, 802.11g o 802.11n. El usuario también puede seleccionar el modo B+G+N para permitir que el router seleccione entre las conexiones 802.11b, 802.11g y 802.11n automáticamente.
Channel Number	El canal utilizado por la red inalámbrica LAN. Todos los dispositivos que estén en la misma red inalámbrica LAN deben usar el mismo canal.
MAC address	Si el usuario desea conectar más de una red a la vez con la red inalámbrica LAN, es necesario configurar este punto de acceso en los siguientes modos: “AP Bridge-Point to Point mode”, “AP Bridge-Point to Multi-Point mode” o “AP Bridge-WDS mode”. Los usuarios tienen que ingresar las direcciones MAC de otros puntos de acceso que se unan a esta tarea.
Set Security	Haga clic en el botón **<Set Security>** para que aparezca la ventana “Security Settings”. Los usuarios pueden configurar los parámetros de seguridad utilizados para unir los puntos de acceso cuando el AP está en modo AP Bridge.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

Modo: AP Bridge – Universal Repeater

En este modo, el router puede funcionar como un repetidor inalámbrico; puede ser Station y AP a la vez. Puede usar la función Station para conectarse a un Root AP y usar la función AP para emitir señal a las estaciones inalámbricas dentro de su área de cobertura.

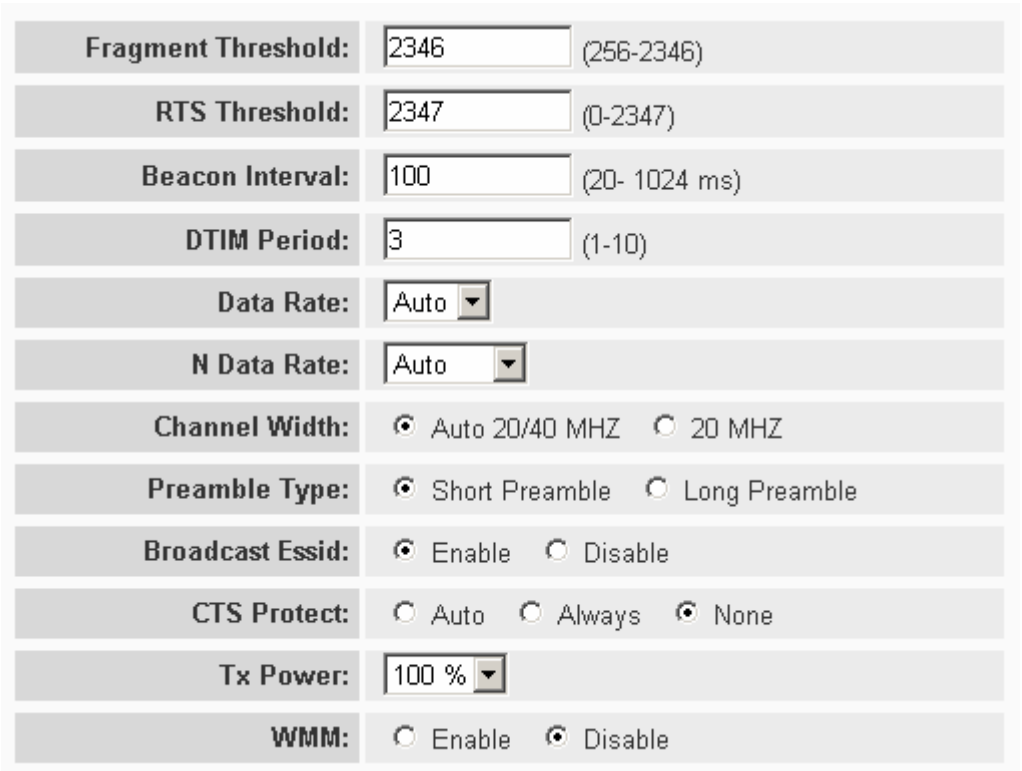


Parámetro	Descripción
Mode	Le permite al usuario configurar los siguientes modos: AP, Station, Bridge o WDS.
Band	Le permite al usuario configurar el modo AP para que quede fijo en 802.11b, 802.11g o 802.11n. Los usuarios también pueden seleccionar el modo B+G+N para que el router elija entre las conexiones 802.11b, 802.11g o 802.11n automáticamente.
ESSID	Este es el nombre de la red inalámbrica LAN. Todos los dispositivos que estén en la misma red inalámbrica LAN deben tener el mismo ESSID.
Channel Number	El canal utilizado por la red inalámbrica LAN. Todos los dispositivos que estén en la misma red inalámbrica LAN deben utilizar el mismo canal.
Associate Clients	Haga clic en el botón <**Show Active Clients**>, luego aparecerá “Active Wireless Client Table”. Los usuarios pueden ver el estado de todas las estaciones que se están conectando al punto de acceso.

Root AP SSID	En el modo “Universal Repeater”, este dispositivo puede actuar como una estación para conectar al Root AP. Debe asignar el SSID del Root AP aquí o hacer clic en el botón <**Select Site Survey**> para elegir un Root AP.
Site Survey	Cuando el usuario utiliza este router inalámbrico como una estación inalámbrica para que el dispositivo de red Ethernet tenga capacidad inalámbrica, tienen que asociarlo con un punto de acceso que funcione. Haga clic en el botón “Select Site Survey”, luego aparecerá “Wireless Site Survey Table”. Es una lista con todos los puntos de acceso cercanos disponibles. Los usuarios pueden seleccionar un punto de acceso de la lista y se unirá a la red inalámbrica LAN a través de este punto de acceso.

4.2.4.2 Ajustes inalámbricos avanzados

Este


Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20- 1024 ms)
DTIM Period: 3 (1-10)
Data Rate: Auto
N Data Rate: Auto
Channel Width: Auto 20/40 MHZ 20 MHZ
Preamble Type: Short Preamble Long Preamble
Broadcast Essid: Enable Disable
CTS Protect: Auto Always None
Tx Power: 100 %
WMM: Enable Disable

router provee algunos controles avanzados para los parámetros inalámbricos. Si el usuario quiere configurar estos ajustes, por favor haga clic en el menú <**Wireless**> que se encuentra a la izquierda de la interfaz de administración web, y luego haga clic en <**Advanced Settings**>. Se mostrará el siguiente mensaje en el navegador de Internet.

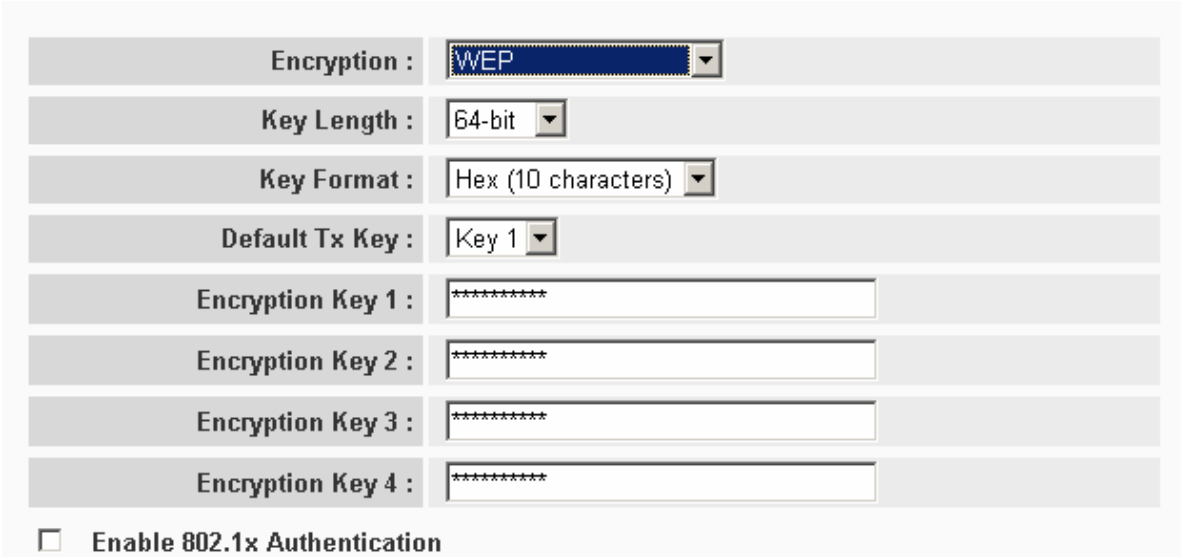
Parámetro	Descripción
Fragment Threshold	"Fragment Threshold" especifica la medida máxima del paquete durante la fragmentación de los datos que se transmitirán. Si los usuarios configuran este valor muy bajo, el resultado será un mal rendimiento. *Default: 2346.*
RTS Threshold	Cuando el tamaño del paquete es más pequeño que el RTS Threshold, el router inalámbrico no utilizará el mecanismo RTS/CTS para enviar este paquete. *Default: 2347*
Beacon Interval	El intervalo de tiempo entre las transmisiones. Los beacon se utilizan para sincronizar la red inalámbrica. *Default: 100*
DTIM Period	Ajusta el período DTIM del radio inalámbrico. *Default: 3*
Data Rate	El "Data Rate" es el índice que este punto de acceso utiliza para transmitir paquetes de datos. El punto de acceso utilizará el índice de transmisión seleccionado más alto posible para transmitir los paquetes de datos.
N Data Rate	El mismo parámetro que el anterior, pero para clientes 802.11n.
Preamble Type	El "Long preamble" puede proporcionar mejor compatibilidad de la red inalámbrica LAN, mientras que el "Short Preamble" puede proporcionar mejor desempeño de la red inalámbrica LAN.
Broadcast ESSID	Si "Broadcast ESSID" está habilitado, cada estación inalámbrica ubicada dentro de la cobertura de este punto de acceso puede descubrir dicho punto de acceso fácilmente. Si los usuarios están construyendo una red inalámbrica pública, se recomienda habilitar esta opción. Deshabilitar "Broadcast ESSID" puede proporcionar mejor seguridad.
CTS Protect	Si habilita esta opción, se reducirá la posibilidad de que haya colisiones de señal de radio entre los puntos de acceso

	inalámbricos 802.11b y 802.11g. Se recomienda configurar esta opción en “Auto” o “Always”.
Tx Power	Los usuarios pueden ajustar la potencia de salida del radio inalámbrico. A menos que el usuario esté utilizando este router inalámbrico en un área verdaderamente grande, no es necesario ajustar la potencia de salida a 100%.
WMM	WMM es la abreviatura de Wi-Fi Multimedia, lo cual mejorará el desempeño de la transferencia de datos de contenidos multimedia cuando se transfieran a través de la red inalámbrica. *Default: “Deshabilitado”*

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.4.3 Seguridad Inalámbrica

Para ajustar las opciones de seguridad inalámbrica, por favor haga clic en el menú <**Wireless**> que se encuentra a la izquierda de la interfaz de administración web y luego



haga clic en <**Security Settings**>. Siga las siguientes instrucciones para ajustar las opciones de seguridad inalámbrica.

Solo WEP

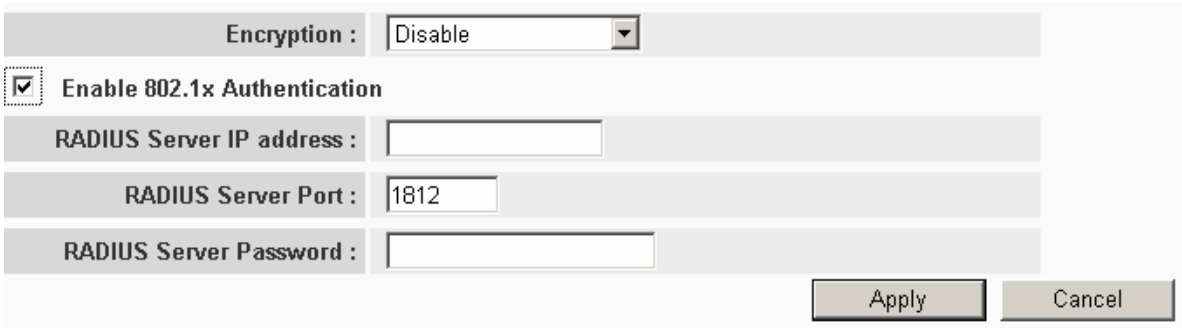
Parámetro	Descripción
Key Lengh	Los usuarios pueden seleccionar la longitud de la clave WEP (WEP key length) para codificar, 64-bit o 128-bit. Las claves WEP más largas proporcionan un nivel mayor de

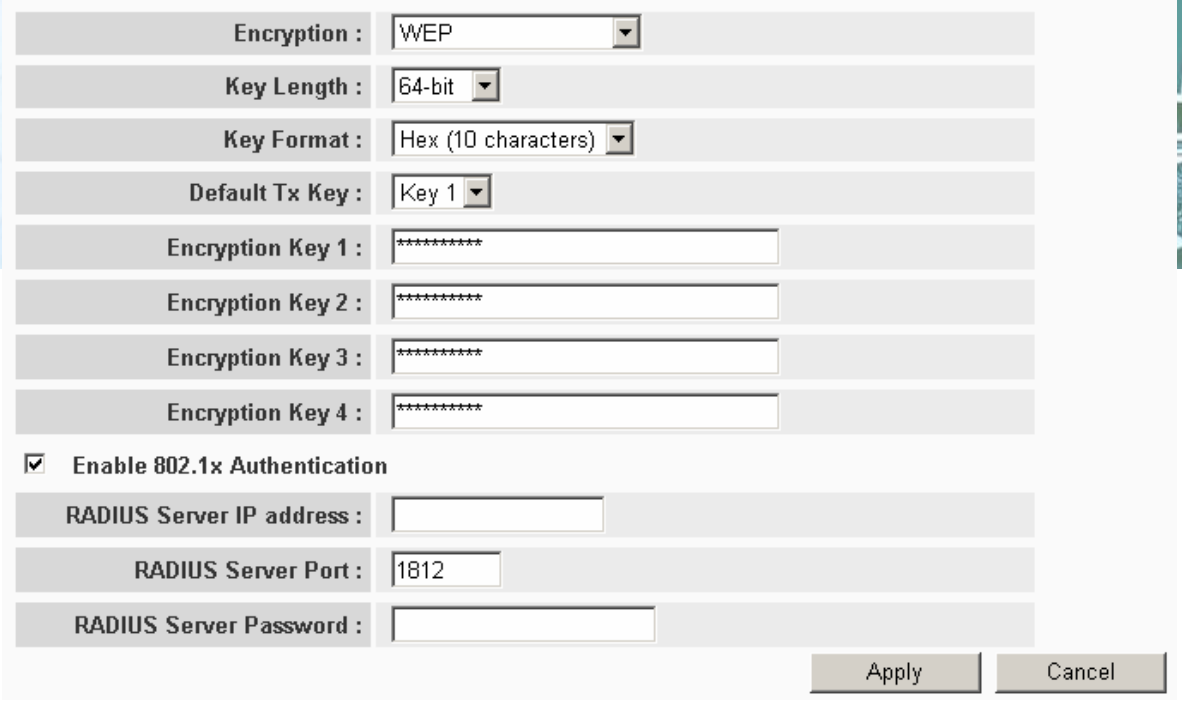
	seguridad, pero el rendimiento será menor. *Default: 64-bit*
Key Format	Hay dos tipos de formato de clave (key format): ASCII y Hexadecimal. Cuando los usuarios seleccionan el formato de una clave, se mostrará el número de caracteres de la clave. Por ejemplo, si los usuarios seleccionan 64-bit como la longitud de la clave y Hex como el formato de la clave, el mensaje a la derecha de "Key Format" será "Hex (10 characters), lo que significa que la longitud de la clave WEP es de 10 caracteres.
Default Key	Seleccione una de las cuatro claves para codificar la información. Solo la clave seleccionada en "Default Key" tendrá efecto.
Key 1 – Key 4	Las claves WEP se utilizan para codificar la información transmitida en la red inalámbrica. Llene los espacios de texto siguiendo las instrucciones debajo. • WEP 64-bit: ingrese valores Hexadecimales de 10 dígitos (en los rangos "A-F, "a-f" y "0-9") o caracteres ASCII de 5 dígitos como las claves de codificación. • WEP 128-bit: ingrese valores Hexadecimales de 26 dígitos (en los rangos "A-F, "a-f" y "0-9") o caracteres ASCII de 13 dígitos como las claves de codificación.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

Solo 802.1x

IEEE 802.1x es un protocolo de autenticación y cada usuario debe utilizar una cuenta válida para iniciar una sesión antes de acceder a la red inalámbrica LAN. La autenticación es procesada por un servidor RADIUS. Este modo solo autentica al usuario por IEEE 802.1x, pero no codifica la información durante la comunicación.




Encryption : WEP
Key Length : 64-bit
Key Format : Hex (10 characters)
Default Tx Key : Key 1
Encryption Key 1 : **********
Encryption Key 2 : **********
Encryption Key 3 : **********
Encryption Key 4 : **********
Enable 802.1x Authentication
RADIUS Server IP address :
RADIUS Server Port : 1812
RADIUS Server Password :
Apply
Cancel

Parámetro	Descripción
RADIUS Server IP address	Es la dirección IP de servidor externo RADIUS.
RADIUS Server Port	Es el puerto de servicio del servidor externo RADIUS
RADIUS Server Password	Es la clave utilizada por el servidor externo RADIUS.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

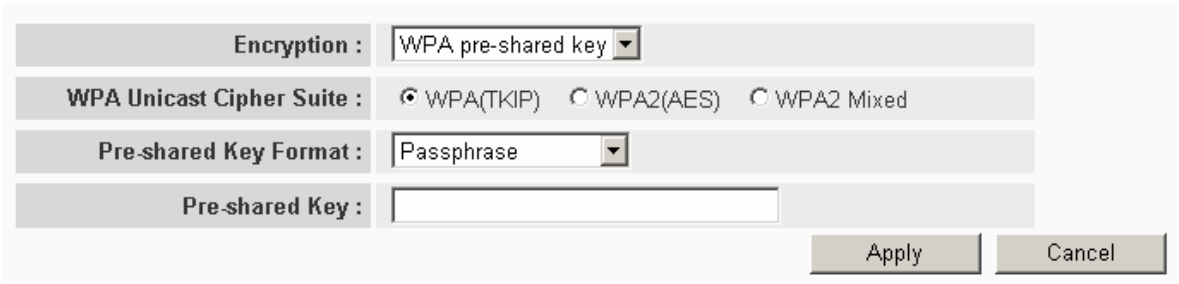
802.1x Clave WEP estática

IEEE 802.1x es un protocolo de autenticación y cada usuario debe utilizar una cuenta válida para iniciar una sesión antes de acceder a la red inalámbrica LAN. La autenticación es procesada por un servidor RADIUS. Este modo también utiliza WEP para codificar la información durante la comunicación.

Remítase a las secciones relevantes para las configuraciones WEP y 802.1x.

Clave pre compartida de WPA

WPA (Wi-Fi Protected Access - Acceso Protegido Wi-Fi) es un estándar de seguridad avanzado. Los usuarios pueden utilizar una clave pre compartida para autenticar las estaciones inalámbricas y codificar la información durante la comunicación. Utiliza TKIP o CCMP (AES) para modificar la clave de codificación con frecuencia. Por lo tanto, la clave de codificación no es fácil de descifrar por los hackers.

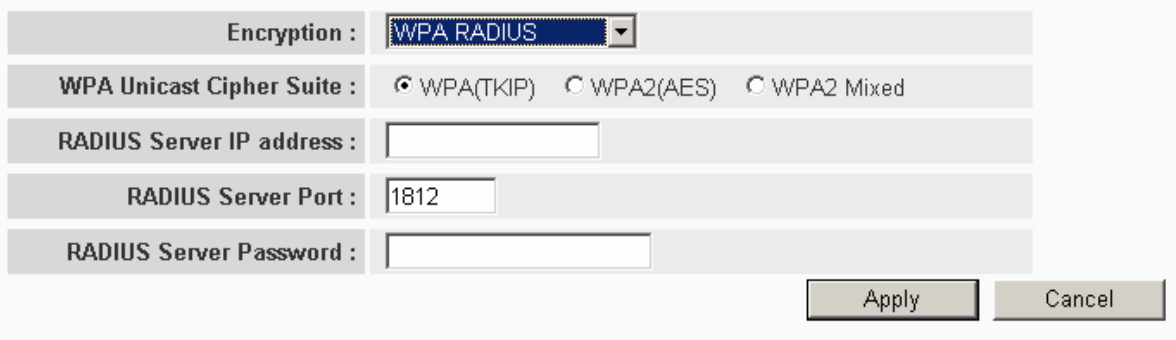


Parámetro	Descripción
WPA(TKIP)	TKIP puede modificar con frecuencia la clave de codificación para mejorar la seguridad de la red inalámbrica LAN.
WPA2(AES)	Utiliza el protocolo CCMP para modificar con frecuencia la clave de codificación. AES puede ofrecer un alto nivel de codificación para mejorar la seguridad inalámbrica de la red inalámbrica LAN.
WPA2 Mixed	Utilizará TKIP o AES basándose en el otro par de comunicación automáticamente.
Pre-shared Key Format	Los usuarios pueden seleccionar una Frase Contraseña (formato alfanumérico) o Dígitos Hexadecimales (en el rango “A-F”, “a-f” y “0-9”) para la clave pre compartida. *Por ejemplo:* *Frase contraseña: iamguest* *Dígitos Hexadecimales: 12345abcde*
Pre-shared Key	La clave pre compartida se utiliza para autentificar y codificar datos transmitidos en la red inalámbrica. Llene el cuadro de texto siguiendo las instrucciones a continuación. WEP Hexadecimal: ingrese 64 dígitos Valores Hexadecimales (en el rango “A-F”, “a-f” y “0-9”) o una frase contraseña de al menos 8 caracteres como las claves per compartidas.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

Radius WPA

WPA (Wi-Fi Protected Access - Acceso Protegido Wi-Fi) es un estándar de seguridad avanzado. Los usuarios pueden utilizar un servidor RADIUS externo para autenticar las estaciones inalámbricas y proporcionar la clave de la sesión para codificar información durante la comunicación. Utiliza TKIP o CCMP (AES) para modificar la clave de codificación con frecuencia.

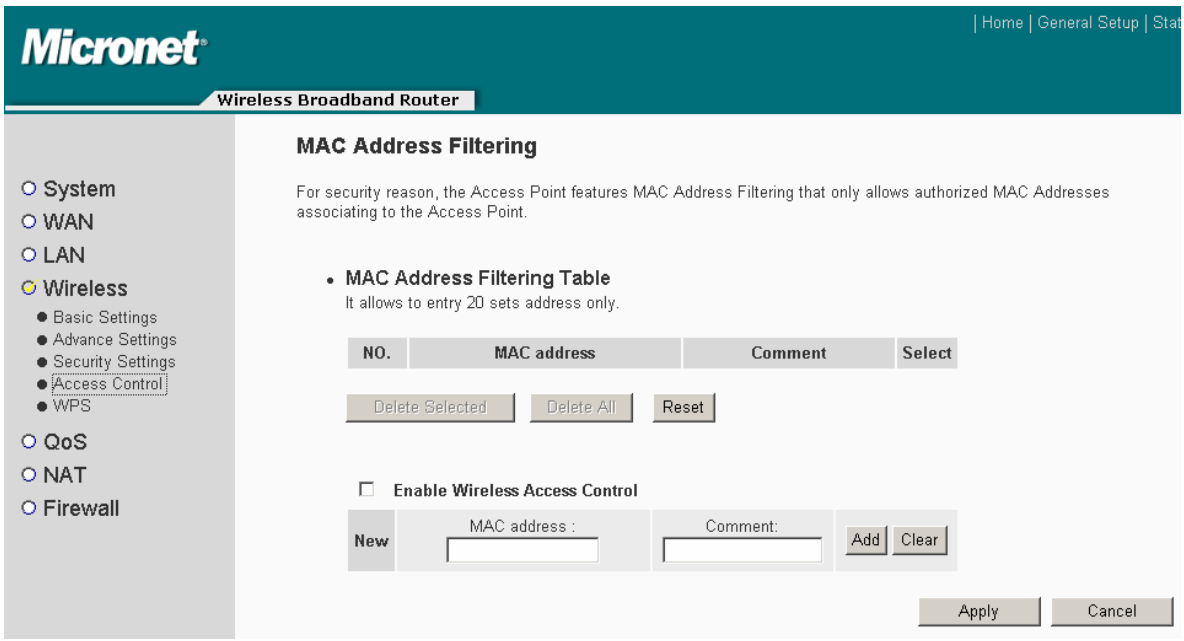


Parámetro	Descripción
WPA(TKIP)	TKIP puede modificar con frecuencia la clave de codificación para mejorar la seguridad de la red inalámbrica LAN.
WPA2(AES)	Utiliza el protocolo CCMP para modificar con frecuencia la clave de codificación. AES puede ofrecer un alto nivel de codificación para mejorar la seguridad inalámbrica de la red inalámbrica LAN.
WPA2 Mixed	Utilizará TKIP o AES basándose en el otro par de comunicación automáticamente.
RADIUS Server Port	Es el puerto de servicio del servidor externo RADIUS. *Default: 1812*
RADIUS Server Password	Es la contraseña utilizada por el servidor externo RADIUS.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.4.4 Control de acceso inalámbrico

Este router inalámbrico posee Control de Direcciones MAC, lo cual evita que las direcciones MAC no autorizadas puedan acceder a la red inalámbrica.

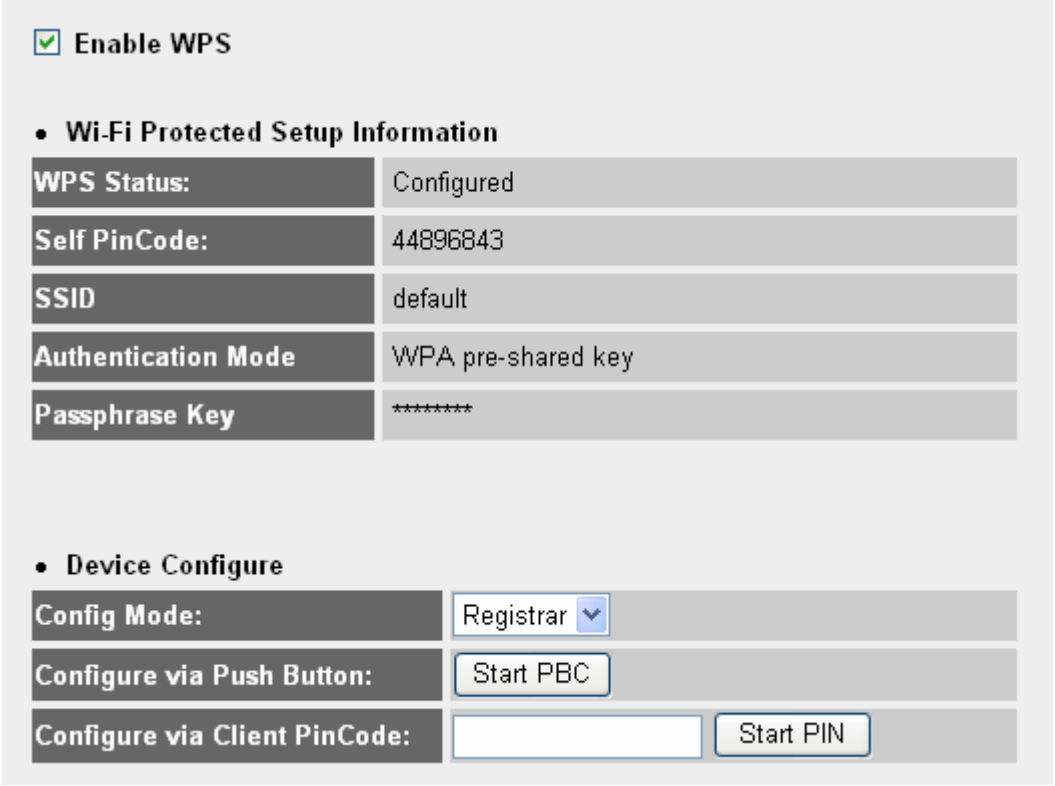


Parámetro	Descripción
Enable wireless access control	Habilita el control de acceso para la conexión inalámbrica.
Add MAC address into the list	Complete los espacios “MAC Address” y “Comment” de la estación inalámbrica que será agregada. Haga clic en <**Add**> para agregar dicha estación a “Current Access Control List”. Haga clic en <**Clear**> para borrar los campos “MAC Address” y “Comment”.
Remove MAC address from the list	Si los usuarios quieren eliminar una dirección MAC de “Current Access Control List”, seleccione la dirección MAC que desea borrar y haga clic en <**Delete Selected**>. Haga clic en el botón <**Delete All**> para eliminar todas las direcciones MAC. Haga clic en <**Reset**> para borrar las selecciones actuales.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.4.5 WPS

WPS (Wi-Fi Protected Setup) es la forma más simple de construir una conexión entre clientes de red inalámbrica y el router inalámbrico. Los usuarios no tienen que seleccionar un modo de codificación e ingresar largas frases contraseña cada vez que configuran un cliente inalámbrico. Este router inalámbrico admite dos tipos de WPS: Push-Button Configuration (PBC) y código PIN. Si los usuarios quieren utilizar PBC, es necesario presionar un botón específico en el cliente inalámbrico para iniciar el modo WPS y cambiar este router inalámbrico a modo WPS también. Puede presionar el botón Reset/WPS en el router o hacer clic en el botón “Start PBC” en la interfaz de configuración de la web. Si los usuarios quieren utilizar el código PIN, es necesario conocer el código PIN del cliente inalámbrico y cambiar a modo WPS, luego debe proporcionar el código PIN del cliente inalámbrico para conectarse a este router. Las instrucciones detalladas se encuentran a continuación:

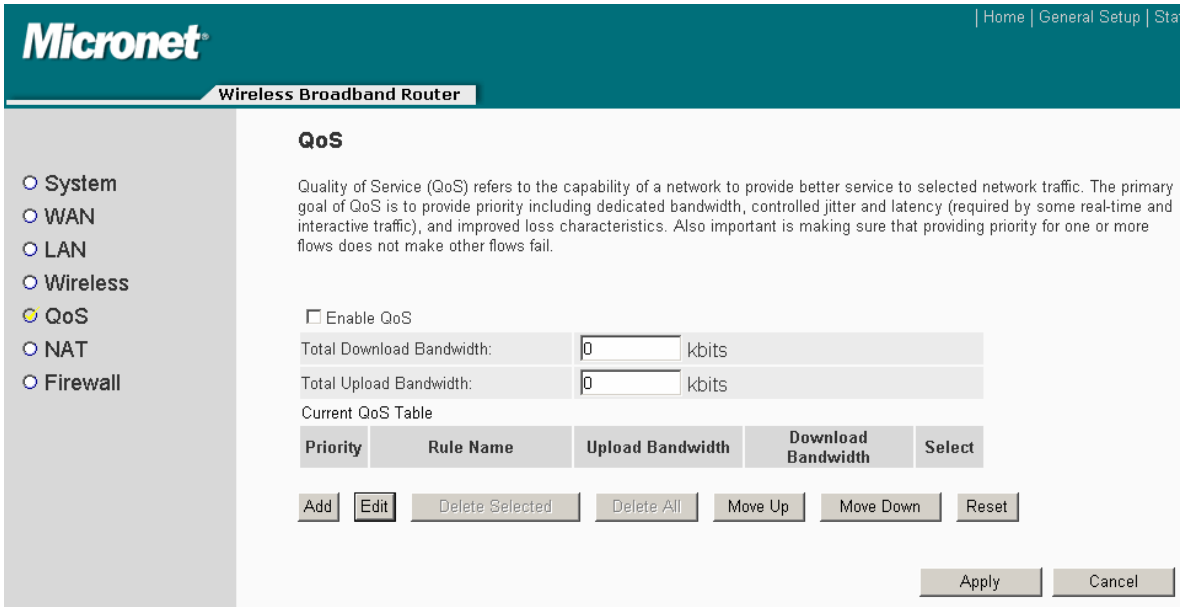


Por favor, haga clic en el menú <**Wireless**> que se encuentra a la izquierda de la interfaz de administración web y haga clic en “**WPS**”. Aparecerá el siguiente mensaje en el navegador de Internet.

Parámetro	Descripción
Enable WPS	Seleccione este recuadro para habilitar la función WPS. Quite la selección para deshabilitar WPS.
WPS Status	Si la función de seguridad inalámbrica (codificación) de este router está ajustada apropiadamente, los usuarios verán el mensaje “Configured”.
Self PIN code	Es el código PIN de WPS de este router. Este código es útil cuando los usuarios necesitan construir conexiones inalámbricas a través de WPS con otros dispositivos inalámbricos que admiten WPS.
SSID	El SSID de este router inalámbrico se mostrará aquí.
Authentication Mode	El modo de autenticación de seguridad inalámbrica de este router se mostrará aquí.
Configure via Push Button	Haga clic en <**Start PBC**> para iniciar el estilo Push-Button de WPS a través del procedimiento de ajuste de Push Button. El router esperará los pedidos WPS de los clientes inalámbricos durante dos minutos. El “WLAN” LED del router se mantendrá fijo cuando el router esté esperando el ingreso de pedidos WPS.
Configure via Client Pin Code	Por favor, ingrese el código PIN del cliente inalámbrico que desea conectar y haga clic en el botón <**Start PIN**>. El “WLAN” LED del router se mantendrá fijo cuando el router esté esperando el ingreso de pedidos WPS.

4.2.5 Q o S

La calidad de servicio (Q o S) brinda una forma eficiente para que las computadoras que están en la red compartan el ancho de banda de Internet con una buena calidad de servicio de Internet. Sin QoS, todas las computadoras y los dispositivos en la red competirán entre ellos para obtener ancho de banda, y algunas aplicaciones que requieren ancho de banda garantizado (como video streaming o teléfonos en red) se verán afectadas. Por lo tanto, habrá un resultado desagradable, como la interrupción de la transferencia de video/ audio.

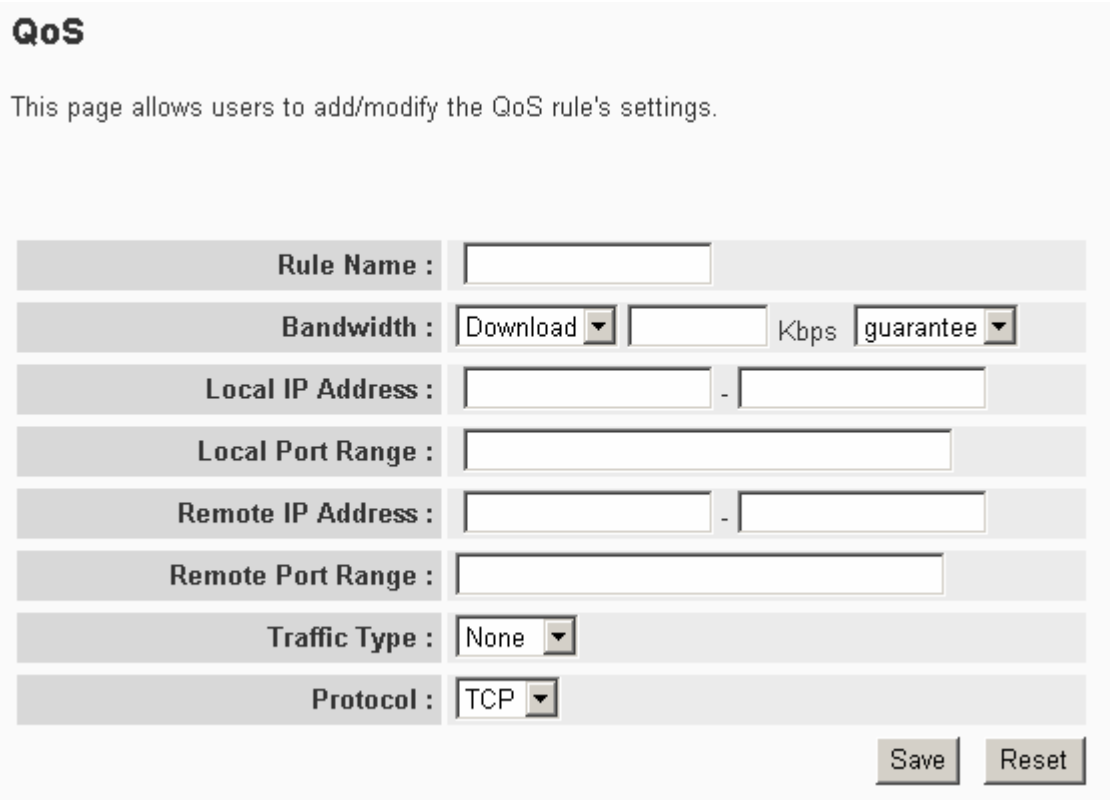


Parámetro	Descripción
Enable/Disable QoS	Permite habilitar o deshabilitar la función QoS.
Add a QoS rule into the table	Haga clic en <**Add**> para ingresar a la página del formulario de las normas de QoS. Haga clic en <**Apply**> después de llenar el formulario y la norma se agregará a la tabla.
Remove QoS rules from the table	Si quiere eliminar las normas de QoS de la tabla, seleccione las normas de QoS y haga clic en <**Delete Selected**>. Para eliminar todas las normas de QoS de la tabla, haga clic en el botón <**Delete All**>. Haga clic en <**Reset**> para borrar las selecciones actuales.
Edit a QoS rule	Seleccione la norma que quiera editar y haga clic en <**Edit**>, luego ingresará el formulario de detalles de la norma QoS. Haga clic en <**Apply**> después de editar el

	formulario y la norma se guardará.
Adjust QoS rule priority	Los usuarios pueden seleccionar la norma y hacer clic en <**Move up**> para darle mayor prioridad. Seleccione la norma y haga clic en <**Move Down**> para darle menor prioridad.

4.2.5.1 Editar normas QoS

Los usuarios pueden asignar paquetes de criterio de clasificación a través de los parámetros de su rango IP local, rango IP remoto, tipo de tráfico, protocolo, rango de puerto local y rango de puerto remoto. Los parámetros que los usuarios dejen en blanco serán ignorados. La prioridad de esta norma será aplicada a paquetes que coincidan con el criterio de clasificación de dicha norma. Puede limitar el ancho de banda consumido por paquetes que coinciden con esta norma o garantizar el ancho de banda requerido por paquetes que coinciden con esta norma.



Parámetro	Descripción
Rule Name	El nombre de esta norma.
Bandwidth	Los usuarios pueden asignar el ancho de banda para descarga o carga en la unidad de Kbps (1024 bit por segundo). Puede

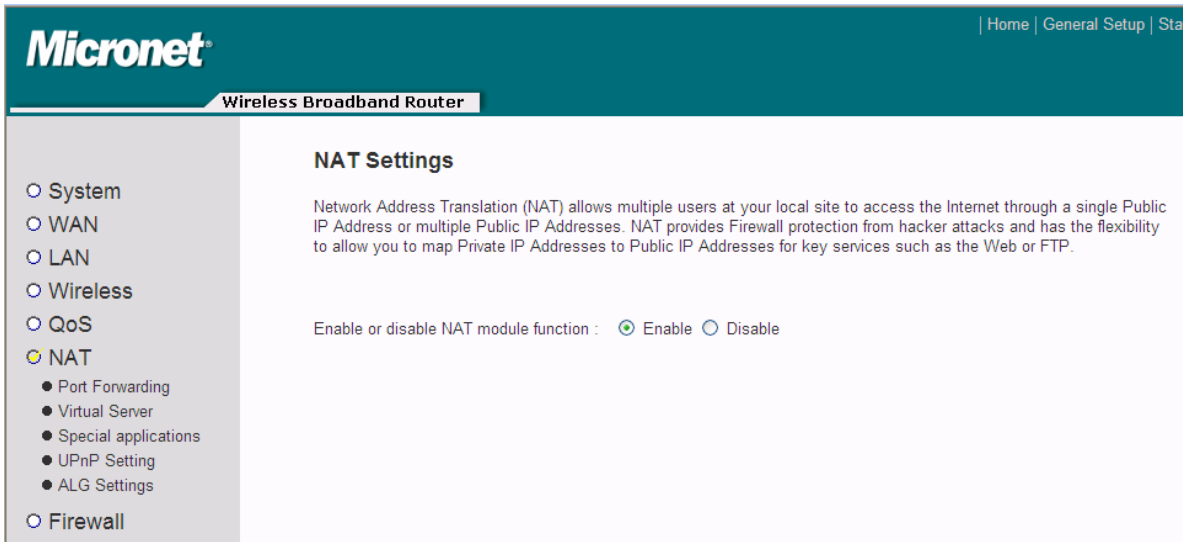
	limitar el máximo de ancho de banda consumido por esta norma seleccionando “Maximum”. Reserve suficiente ancho de banda para esta norma seleccionando “Guarantee”.
Local IP Address	Ingrese el rango de dirección IP local de los paquetes que aplicarán esta norma. Si los usuarios asignan 192.168.2.3 – 192.168.2.5, significa tres direcciones IP: 192.168.2.3, 192.168.2.4 y 192.168.2.5.
Local Port Range	Ingrese el rango de puerto local de los paquetes que aplicarán esta norma. Los usuarios pueden asignar un solo número de puerto aquí o un rango de números de puerto asignando el primer número de puerto y el último número de puerto del rango. Los dos números están separados por un guión “-“, por ejemplo “100-150” significa que el rango va desde el número de puerto 100 hasta el 150 – el rango de 50 números de puerto.
Remote IP Address	Ingrese el rango de direcciones IP remotas de los paquetes que aplicarán esta norma. Si los usuarios asignan 192.168.2.3 – 192.168.2.5, significa tres direcciones IP: 192.168.2.3, 192.168.2.4 y 192.168.2.5.
Remote Port Range	Ingrese el rango de puerto remoto de los paquetes que aplicarán esta norma. Los usuarios pueden asignar un solo número de puerto aquí o un rango de números de puerto asignando el primer número de puerto y el último número de puerto del rango. Los dos números están separados por un guion “-“, por ejemplo “100-150” significa que el rango va desde el número de puerto 100 hasta el 150 – el rango de 50 números de puerto.
Traffic Type	Seleccione el tipo de tráfico de los paquetes que aplicarán esta norma. Hay una lista de algunas aplicaciones populares disponible para facilitar la configuración. Los usuarios también pueden obtener los mismos resultados utilizando otros parámetros.
Protocol	Seleccione el tipo de protocolo de los paquetes que aplicarán esta norma.
Save	Guarda el formulario y sale de éste.
Reset	Borra el contenido de este formulario.

*Haga clic en el botón <**Save**> en la parte inferior de la pantalla para guardar las configuraciones modificadas.*

4.2.6 NAT

NAT (Network Address Translation - Traducción de Dirección de Red) soluciona el problema de compartir una sola dirección IP con múltiples computadoras. Sin NAT, todas las

computadoras deben tener asignadas una dirección IP de Internet válida. Por lo tanto, es necesario utilizar la tecnología NAT para compartir una sola dirección IP de Internet con múltiples computadoras en la red local, para que todos puedan conectarse a Internet.

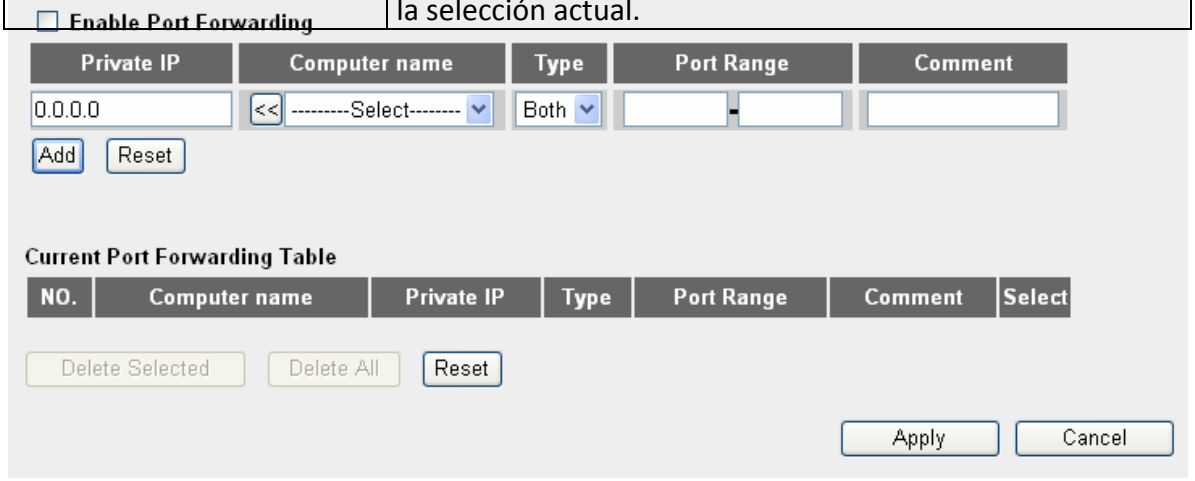

Micronet
Wireless Broadband Router
| Home | General Setup | Sta
System
WAN
LAN
Wireless
QoS
NAT
Port Forwarding
Virtual Server
Special applications
UPnP Setting
ALG Settings
Firewall
NAT Settings
Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as the Web or FTP.
Enable or disable NAT module function : Enable Disable

4.2.6.1 Redirección de puerto (Port Forwarding)

Esta función le permite al usuario redirigir un solo puerto o puertos consecutivos de la dirección IP de Internet al mismo puerto de la dirección IP de la red local. El/los número(s) de puerto de la dirección de IP de Internet y la dirección IP privada (la dirección IP de la red local) debe(n) ser el/los mismo(s). Si el número de puerto de la dirección IP de Internet y la dirección IP privada es diferente, por favor utilice la función “Virtual Server” que se describe en la siguiente sección.

Parámetro	Descripción
Enable Port Forwarding	Permite que se habilite la redirección de puerto.
Private IP	Éste es el IP privado del servidor detrás del firewall de NAT. Los usuarios tendrán que darles a los clientes de LAN PC una dirección IP fija/estática para que la redirección de puerto funcione apropiadamente.
Computer Name	Abra el menú y verá listadas aquí todas las computadoras conectadas al router. Los usuarios pueden seleccionar fácilmente el nombre de la computadora sin revisar la dirección IP de la computadora.
Type	Éste es el tipo de protocolo que será redireccionado. Los usuarios pueden elegir redireccionar paquetes “TCP” o “UDP” solamente o pueden seleccionar “both” para redireccionar ambos paquetes.
Port Range	El rango de puertos que será redireccionado al IP privado.

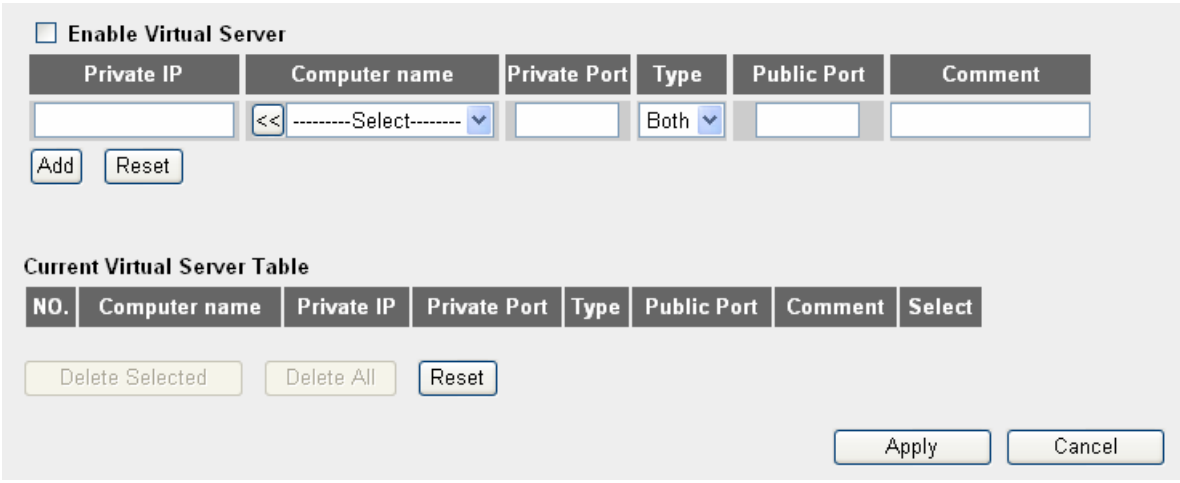
Comment	Es la descripción de este ajuste.
Add Port Forwarding into the table	Complete los campos “Private IP”, “Type”, “Port Range” y “Comment” en el ajuste y haga clic en <**Add**>. Este ajuste de Port Forwarding será agregado a la “Current Port Forwarding Table”. Haga clic en <**Reset**> para vaciar los campos.
Remove Port Forwarding into the table	Si los usuarios quieren eliminar algunos ajustes de Port Forwarding de la “Current Port Forwarding Table”, deben seleccionar el ajuste de Port Forwarding y hacer clic en <**Delete Selected**>. Haga clic en el botón <**Delete All**> para eliminar todos los ajustes. Haga clic en <**Reset**> para borrar la selección actual.



*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.6.2 Servidor virtual (Virtual Server)

Esta función le permite al usuario redireccionar un puerto en una dirección IP de Internet (en puerto WAN) a un puerto especificado de una dirección IP en la red local, para que pueda establecer un servicio de Internet en la computadora en la red local, sin exponerla directamente en Internet. Los usuarios también pueden construir muchas series de redirección de puerto para proporcionar muchos servicios de Internet diferentes en distintas computadoras locales a través de una sola dirección IP de Internet.



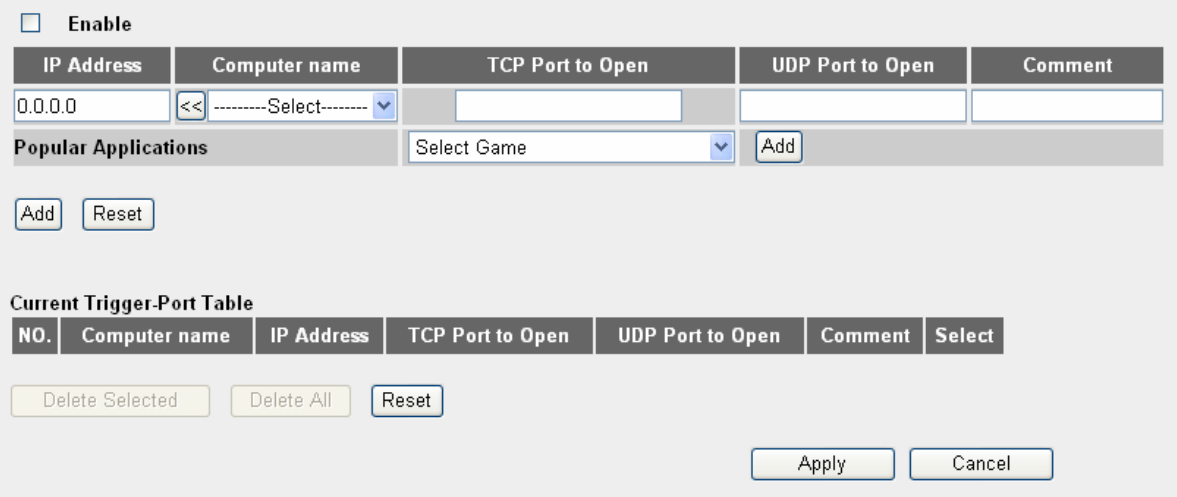
Parámetro	Descripción
Enable Virtual Server	Permite que se habilite el Servidor Virtual.
Private IP	Ésta es la dirección IP del cliente/host LAN que enviará el paquete del número de Puerto Público. Los usuarios tendrán que darles a los clientes de LAN PC una dirección IP fija/estática para que la redirección de puerto funcione apropiadamente.
Computer Name	Abra el menú y verá listadas aquí todas las computadoras conectadas al router. Los usuarios pueden seleccionar fácilmente el nombre de la computadora sin revisar la dirección IP de la computadora.
Private Port	Éste es el número de puerto (del host de IP Privado mencionado anteriormente) al que cambiará el número de Puerto Público mencionado debajo cuando el paquete ingrese la LAN (al Servidor/ Cliente IP LAN).
Type	Seleccione el tipo de protocolo del número de puerto (TCP, UDP o ambos). Si los usuarios no están seguros, pueden dejarlo en default.
Public Port	Ingrese desde Internet el número de puerto del servicio (servicio/ aplicación de Internet) que será redirigido al host de la dirección IP Privada en la LAN. La función Virtual Server tendrá prioridad sobre la función DMZ si

	hubiera un conflicto entre los ajustes del Virtual Server y el DMZ.
Comment	Es la descripción de este ajuste.
Add Virtual Server	Complete los campos “Private IP”,”Private Port” “Type”, “Public Port” y “Comment” en el ajuste y haga clic en <**Add**>. Este ajuste de Virtual Server será agregado a la “Current Virtual Server Table”. Haga clic en <**Reset**> para vaciar los campos.
Remove Virtual Server	Si los usuarios quieren eliminar algunos ajustes de Virtual Server de la “Current Virtual Server Table”, deben seleccionar el ajuste de Virtual Server y hacer clic en <**Delete Selected**>. Haga clic en el botón <**Delete All**> para eliminar todos los ajustes. Haga clic en <**Reset**> para borrar la selección actual.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.6.3 Mapeo de puertos para aplicaciones especiales

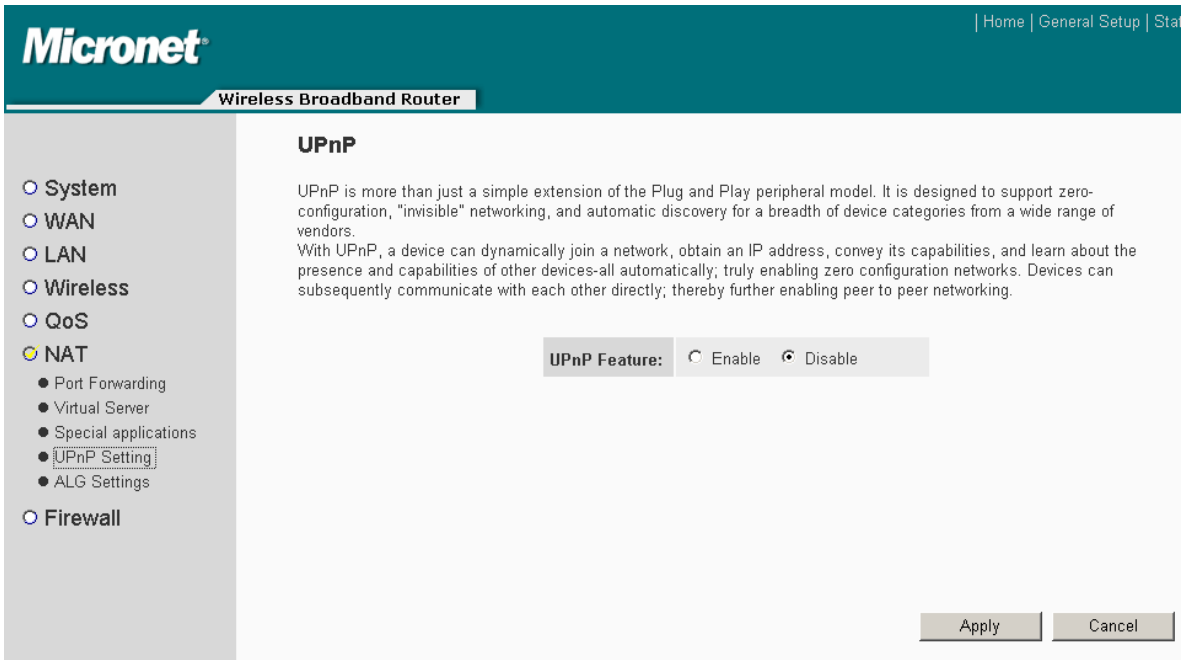
Algunas aplicaciones requieren más de una conexión al mismo tiempo y no funcionan con simples normas NAT. Para hacer que estas aplicaciones funcionen, los usuarios pueden utilizar esta función para que las aplicaciones operen apropiadamente.



4.2.6.4 Ajustes para UPnP

Esta función permite la auto configuración de la red para las comunicaciones puerto a puerto. Los dispositivos de red podrán comunicarse con otros dispositivos directamente y

obtener información sobre dichos dispositivos. En la actualidad, muchos dispositivos y aplicaciones de red confían en la función UPnP.

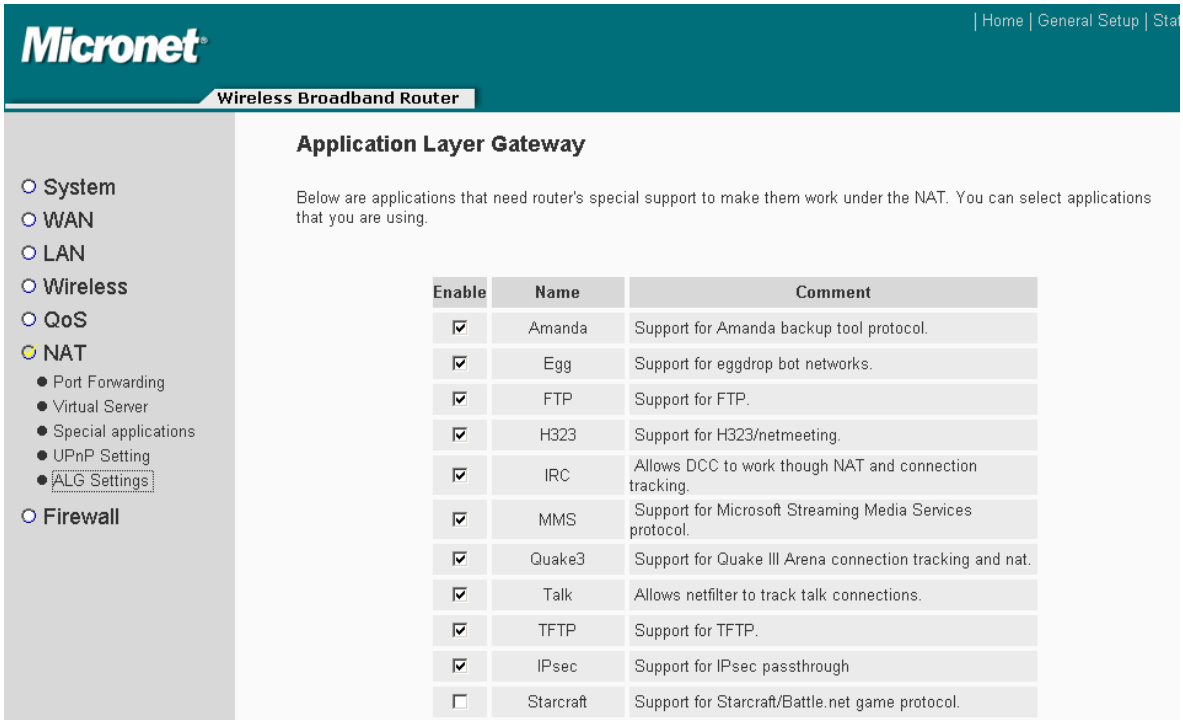

Micronet
Wireless Broadband Router
| Home | General Setup | Sta
System
WAN
LAN
Wireless
QoS
NAT
Port Forwarding
Virtual Server
Special applications
UPnP Setting
ALG Settings
Firewall
UPnP
UPnP is more than just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors.
With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.
UPnP Feature:
Enable
Disable
Apply
Cancel

Parámetro	Descripción
UPnP Feature	Los usuarios pueden habilitar o deshabilitar la función UPnP. Si habilita esta función, todos los sistemas de clientes que admiten UPnP, como Windows XP, pueden encontrar este router automáticamente y acceder a Internet a través de este router sin configuración. La función NAT Traversal que proporciona UPnP permite que las aplicaciones que admiten UPnP se conecten fácilmente a los sitios de Internet sin problemas de incompatibilidad debido a la traducción del puerto NAPT.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.6.5 Ajustes de ALG

Los usuarios pueden seleccionar aplicaciones que necesiten el respaldo de ALG (Application Layer Gateway).

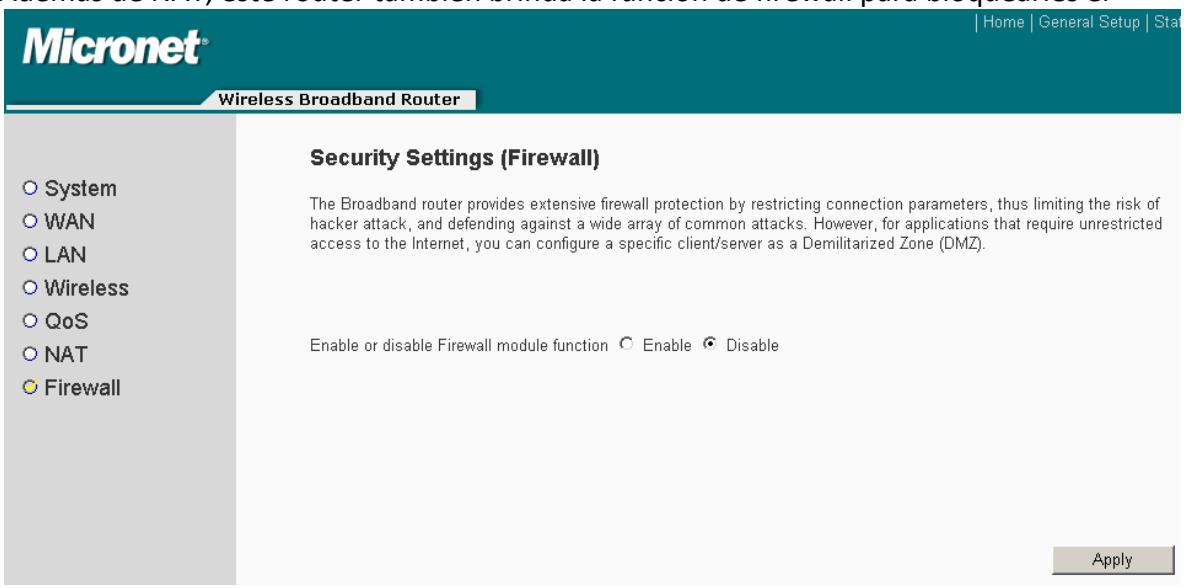


Parámetro	Descripción
Enable	Los usuarios pueden habilitar “Application Layer Gateway” y el router dejará que la aplicación pase correctamente a través del puerto NAT.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.7 Firewall

Además de NAT, este router también brinda la función de firewall para bloquearles el

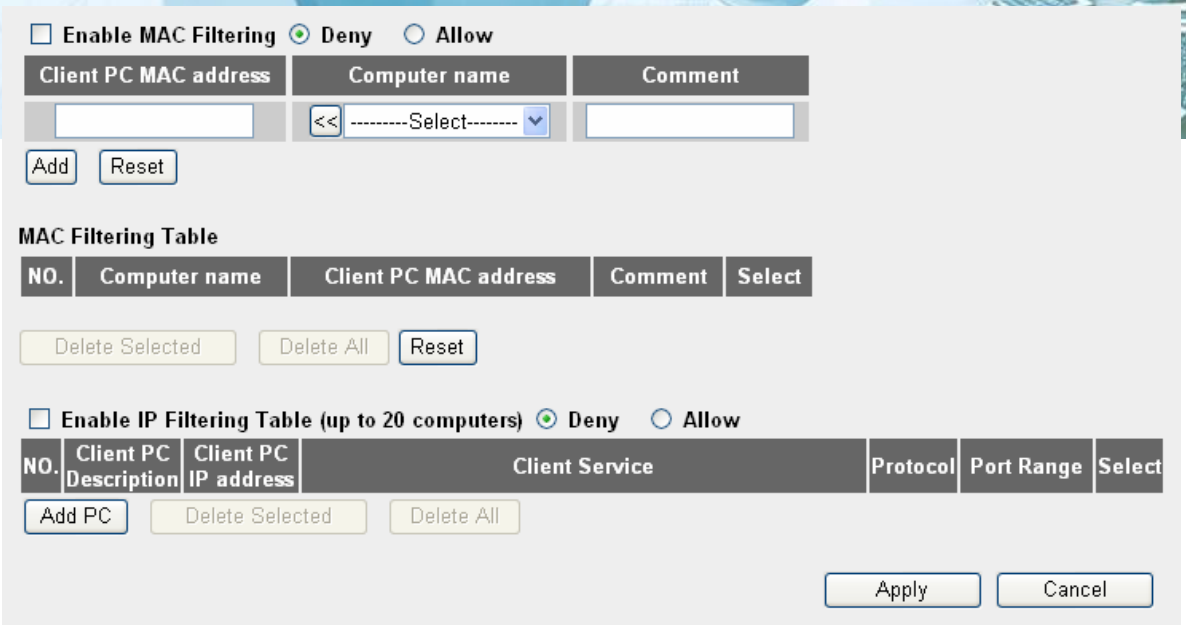

Micronet
Wireless Broadband Router
| Home | General Setup | Sta
System
WAN
LAN
Wireless
QoS
NAT
Firewall
Security Settings (Firewall)
The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).
Enable or disable Firewall module function Enable Disable
Apply

acceso a las computadoras de la red local a los intrusos maliciosos. Estas funciones incluyen prevención de ataques entrantes y bloqueo de tráfico saliente, como el bloqueo de los URL que tienen palabras clave pre definidas.

Parámetro	Descripción
Access Control	Access Control le permite al usuario especificar cuáles son los hosts a los que los usuarios pueden o no tener acceso a ciertas aplicaciones de Internet.
URL Blocking	URL Blocking le permite al usuario especificar cuáles son los URL a los que no se puede acceder.
DoS	El firewall del Broadband router puede bloquear los ataques comunes de los hackers y puede registrar las actividades de los ataques.
DMZ	La función DMZ le permite a los usuarios redirigir todos los paquetes que van de la dirección IP del puerto WAN a una dirección IP particular en su LAN.

4.2.7.1 Control de acceso (Access Control)

Restrinja a los usuarios de acceder a ciertas aplicaciones o ciertos servicios de Internet a través de esta interfaz (Ej.: sitios de Internet, email, FTP, etc). El Control de Acceso les permite a los usuarios definir el tipo de tráfico permitido en la LAN. Los usuarios pueden controlar que cliente PC tiene acceso a estos servicios.

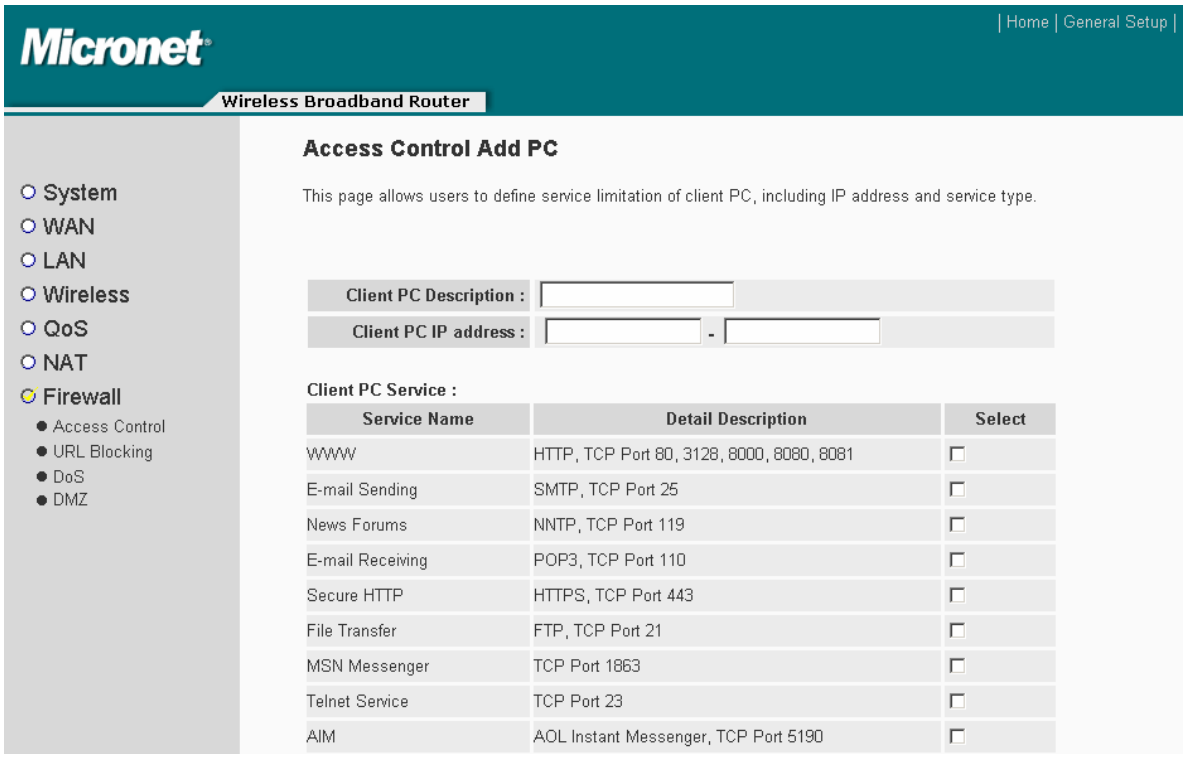


Parámetro	Descripción
Deny	Si selecciona <**Deny**>, todas las PC podrán acceder a Internet, además de las PC en la lista de abajo.
Allow	Si selecciona <**Allow**>, todas las PC no podrán acceder a Internet, excepto las PC en la lista de abajo.
Computer Name	Abra el menú y verá listadas aquí todas las computadoras conectadas al router. Los usuarios pueden seleccionar fácilmente el nombre de la computadora sin revisar la dirección IP de la computadora.
Filter client PCs by IP	Complete “IP Filtering Table” para filtrar los clientes PC por IP.
Add PC	Los usuarios pueden hacer clic en <**Add**> PC para agregar una norma de control de acceso para los usuarios por direcciones IP.
Remove PC	Si los usuarios quieren eliminar algunas PC de la “IP Filtering Table”, deben seleccionar la PC y hacer clic en <**Delete Selected**>. Haga clic en el botón <**Delete All**> para eliminar todas las PC de la tabla.
Comment	Es la descripción de este ajuste.
Filter client PC by MAC address	Seleccione <**Enable MAC Filtering**> para habilitar el filtro de MAC.
Add PC	Complete “Client PC MAC Address” y “Comment” de la PC que tiene permitido acceder a Internet y haga clic en <**Add**>. Haga clic en <Reset> para borrar todos los campos.

Remove PC	Si los usuarios quieren eliminar algunas PC de la “MAC Filtering Table”, deben seleccionar la PC y hacer clic en <**Delete Selected**>. Haga clic en el botón <**Delete All**> para eliminar todas las PC de la tabla. Haga clic en <**Reset**> para borrar todas las selecciones.

Control de acceso – Agregar PC

Después de hacer clic en el botón, el siguiente mensaje aparecerá en el navegador de Internet.



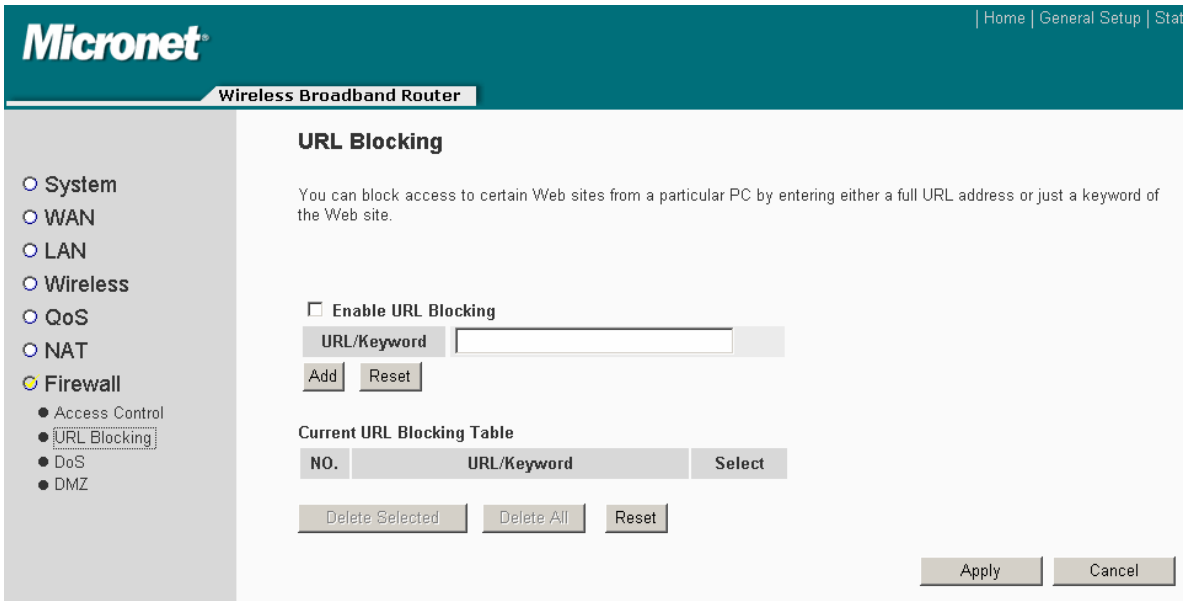
Parámetro	Descripción
Client PC Description	Es la descripción de esta norma de cliente PC.
Client PC IP Addresses	Ingrese el rango de direcciones IP que aplican a esta norma de Access Control. Los usuarios tendrán que darles a los clientes PC LAN una dirección IP fija/estática para que Access Control funcione apropiadamente.
Client PC Service	Los usuarios pueden evitar que los clientes accedan a algunos servicios de Internet seleccionando los servicios que quieren bloquear.
Protocol	Esto les permite a los usuarios seleccionar UDP, TCP o ambos tipos de protocolo para bloquearlos.

Port Range	Se pueden asignar hasta cinco rangos de puerto. El router evitará que los clientes accedan a los servicios de Internet que utilizan estos puertos.
Add	Haga clic en <**Add**> para guardar los ajustes.
Reset	Haga clic en <**Reset**> para borrar todos los campos.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.2.7.2 Bloqueo de URL (URL Blocking)

Los usuarios pueden bloquear el acceso a algunos sitios de Internet de las PC particulares ingresando una dirección de URL completa o simplemente la palabra clave del sitio Web.

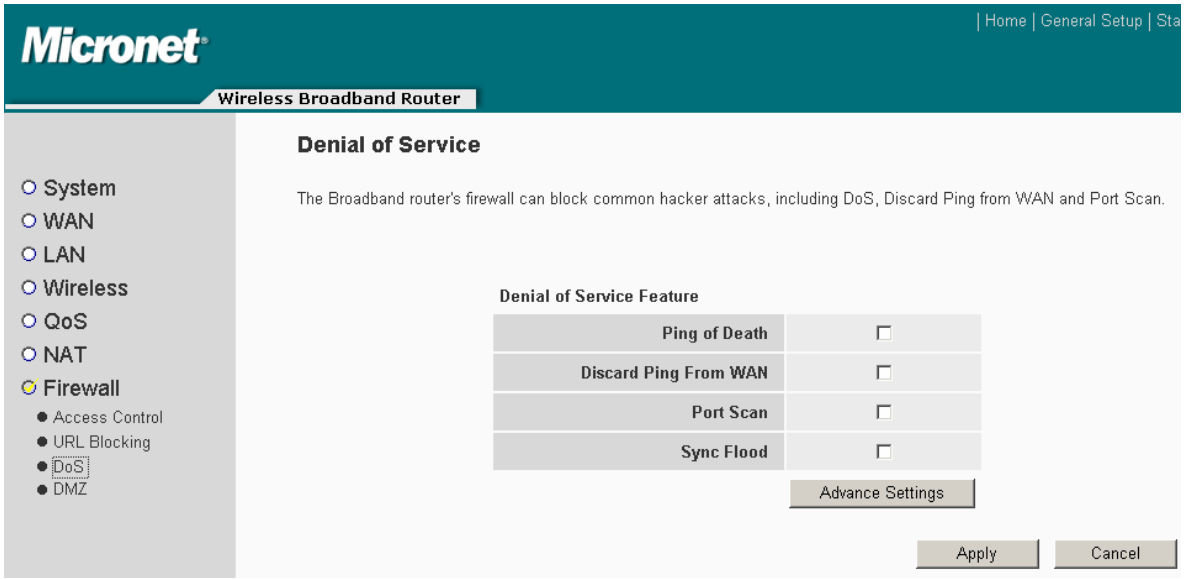


Parámetro	Descripción
Enable URL Blocking	Permite que se habilite la opción URL Blocking.
Add URL Keyword	Complete “URL/Keyword” y luego haga clic en <**Add**>. Los usuarios pueden ingresar la dirección completa del URL o la palabra clave del sitio Web que quieren bloquear. Haga clic en <**Reset**> para borrar todos los campos.
Remove URL Keyword	Si los usuarios quieren eliminar una palabra clave de un URL de la "Current URL Blocking Table", deben seleccionar la palabra clave que quieren eliminar y hacer clic en <**Delete Selected**>. Haga clic en el botón <**Delete**

	All> para eliminar todo lo ingresado. Para borrar la selección, solo haga clic en <**Reset**>.

4.2.7.3 Prevención de ataques DoS (DoS attack)

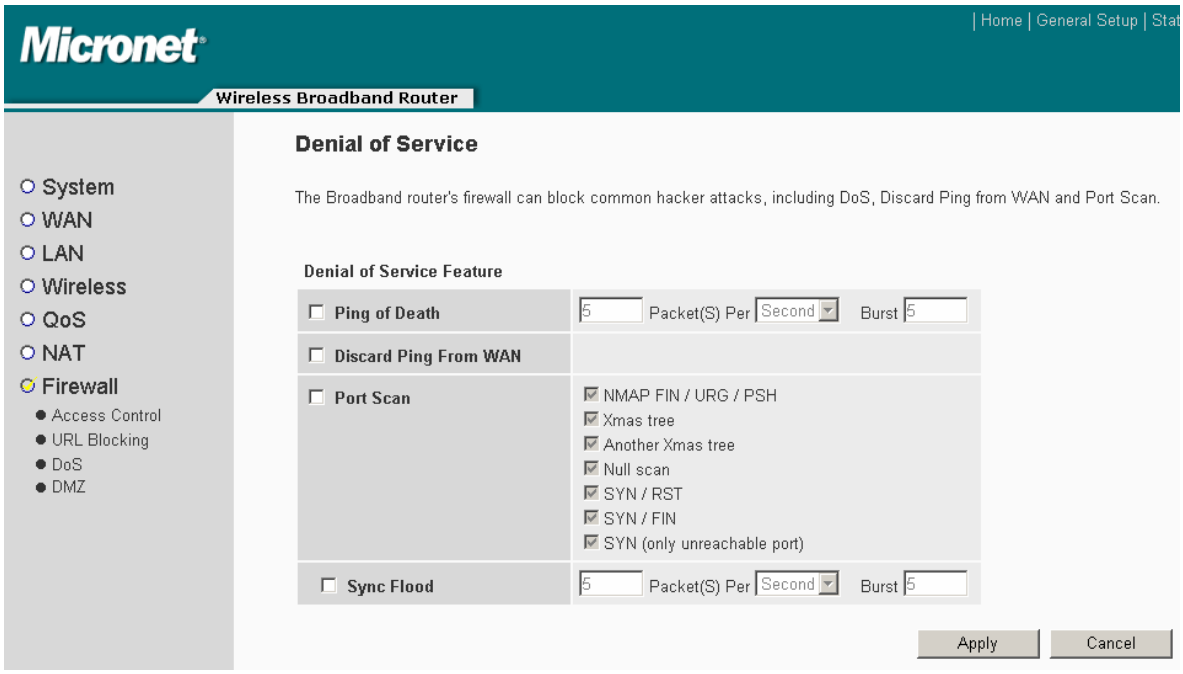
El firewall del Broadband router puede bloquear ataques comunes de hackers, incluyendo Denial of Service, Ping of Death, Port Scan y Sync Flood. Cuando ocurren los ataques de Internet, el router puede registrar los eventos.



Parámetro	Descripción
Ping of Death	Protección contra los ataques Ping of Death.
Discard Ping From WAN	El puerto WAN del router no responderá a ninguna solicitud de Ping.
Port Scan	Protege al router de los escaneos de puertos
Sync Flood	Protege al router de los ataques Sync Flood.
Advanced Settings	Haga clic en este botón para ingresar en la configuración de los ajustes avanzados para el método DoS.

DoS – Ajustes avanzados

Cuando los usuarios hacen clic en el botón **<Advanced Settings>** en el menú DoS, el siguiente mensaje aparecerá en el navegador de Internet.

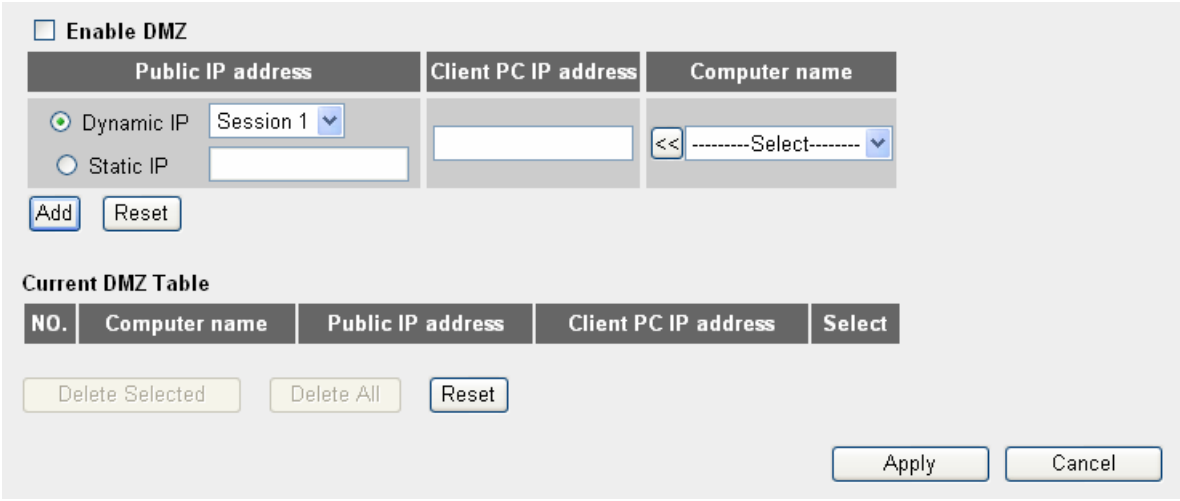


Parámetro	Descripción
Ping of Death	Ajuste el umbral para cuando el mecanismo de prevención DoS será activado. Por favor, seleccione el recuadro Ping of Death e ingrese la frecuencia del umbral (cuantos paquetes por segundo, minuto u hora). Los usuarios también pueden ingresar el valor “Burst”, que significa que cuando este número “Ping of Death” se reciba en un período corto de tiempo, este mecanismo de prevención DoS será activado.
Discard Ping From WAN	Seleccione este recuadro para activar este mecanismo de prevención DoS.
Port Scan	Aquí se listan muchas clases de métodos de escaneo de puertos. Por favor, seleccione uno o más métodos de ataque DoS para que se activen.
Sync Flood	Como con Ping of Death, los usuarios pueden configurar el umbral para cuando este mecanismo de prevención DoS estará activado.

4.2.7.4 Zona desmilitarizada (DMZ)

Si los usuarios tienen un cliente PC local que no puede ejecutar una aplicación de Internet (Ej.: Juegos) apropiadamente debido al firewall NAT, el router puede abrir al cliente a un acceso a Internet de dos direcciones no restringido, definiendo un Host DMZ. La función

DMZ permite la redirección de todos los paquetes que van de la dirección IP de puerto WAN a una dirección IP particular en la LAN. La diferencia entre el servidor virtual y la función DMZ es que el servidor virtual redirige un servicio o una aplicación de Internet particular (ej.: FTP, sitios Web) a un cliente/servidor LAN particular, mientras que DMZ redirige todos los paquetes (sin importar el servicio) que van de su dirección IP WAN a un cliente/servidor LAN particular.



Parámetro	Descripción
Enable DMZ	Permite que se habilite la función DMZ. Si hay un conflicto entre la configuración de Virtual Server y de DMZ, entonces la función Virtual Server tendrá prioridad sobre la función DMZ.
Public IP Address	Es la dirección IP del puerto WAN o cualquier otra dirección IP pública otorgada por el ISP del usuario.
Client PC IP Address	Ingrese la dirección IP de un host particular en la LAN que recibirá todos los paquetes que originalmente vayan al puerto o a la dirección IP pública mencionada anteriormente. Los usuarios tendrán que darles a los clientes PC LAN una dirección IP fija/estática para que DMZ funcione apropiadamente.
Computer Name	Abra el menú y verá listadas aquí todas las computadoras conectadas al router. Los usuarios pueden seleccionar fácilmente el nombre de la computadora sin revisar la dirección IP de la computadora.

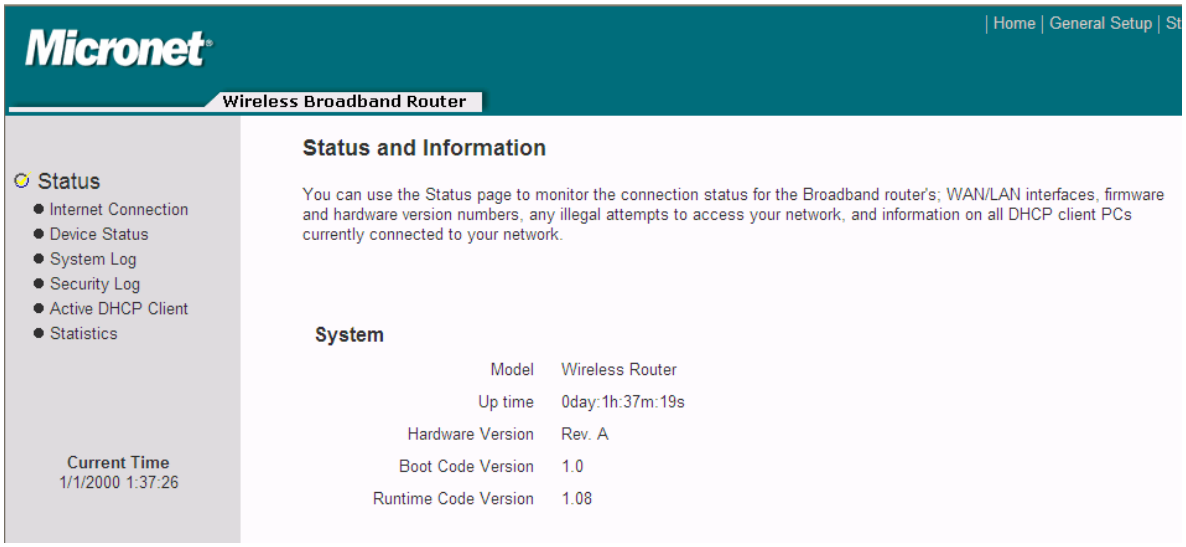
4.3 Estado (Status)

La sección Status le permite al usuario controlar el estado actual del router. Utilice la página de Status para controlar la siguiente información:

- El estado de conexión de las interfaces WAN/LAN del Broadband router.
- Los números de versión actuales del firmware y el hardware.
- Cualquier intento legal de acceder a la red, e información sobre todos los clientes PC DHCP actualmente conectados a la red.

4.3.1 Información del sistema

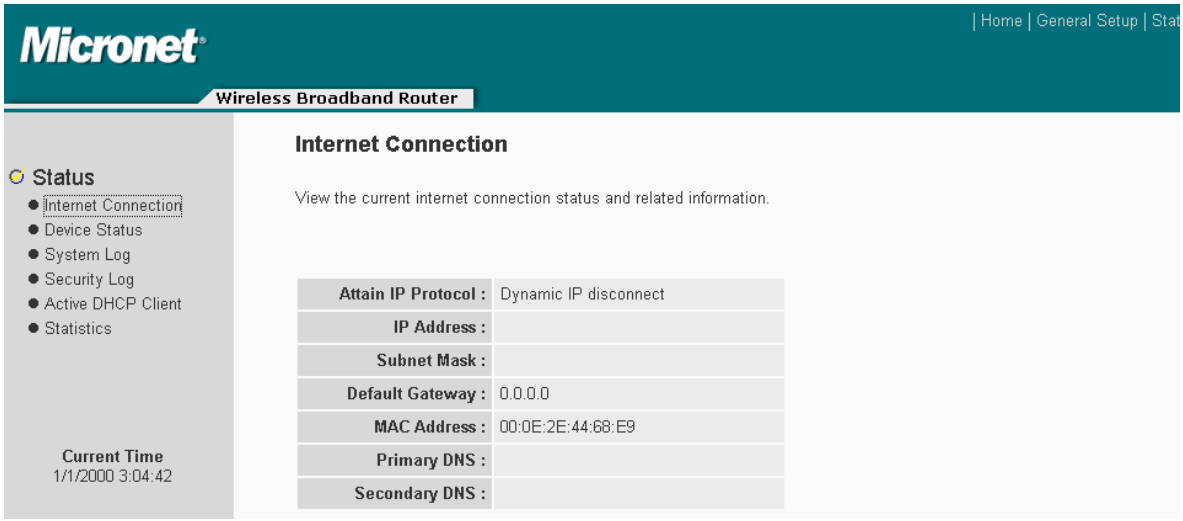
La sección Status and Information (estado e información) le permite al usuario ver la información de sistema del router.


Micronet
Wireless Broadband Router
| Home | General Setup | St
Status
Internet Connection
Device Status
System Log
Security Log
Active DHCP Client
Statistics
Current Time
1/1/2000 1:37:26
Status and Information
You can use the Status page to monitor the connection status for the Broadband router's; WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.
System
Model Wireless Router
Up time 0day:1h:37m:19s
Hardware Version Rev. A
Boot Code Version 1.0
Runtime Code Version 1.08

Parámetro	Descripción
Information	Los usuarios pueden ver la información de sistema del router, tal como la versión del Hardware, el Número de Serie, la versión del Boot code y la versión del Runtime code.

4.3.2 Estado de la conexión de Internet

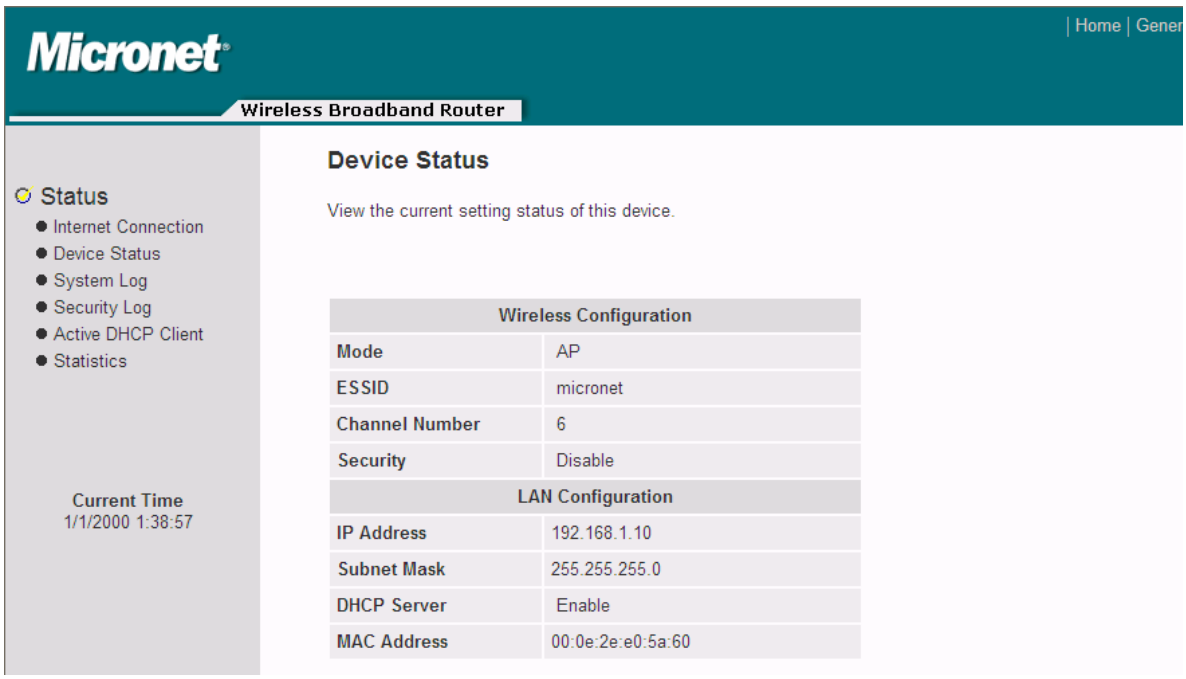
Vea el estado de la conexión de Internet actual del Broadband router y otra información relacionada.



Parámetro	Descripción
Internet Connection	Esta página muestra si el puerto WAN está conectado a una conexión Cable/DSL. También muestra el puerto WAN del router: dirección IP WAN, Subnet Mask y ISP Gateway y también el Primary DNS y el Secondary DNS que se está utilizando.

4.3.3 Estado del dispositivo

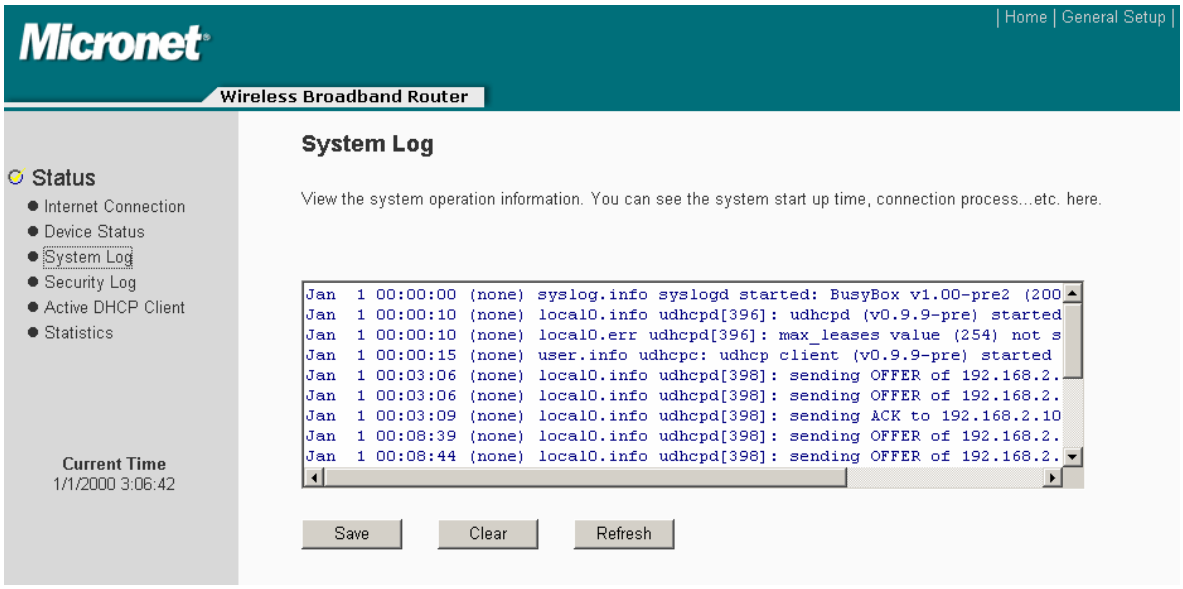
Vea los ajustes de configuración actuales del Broadband router. El Device Status (estado del dispositivo) muestra los ajustes de configuración donde los usuarios han configurado en la sección Quick Setup Wizard/General Setup.



Parámetro	Descripción
Device Status	Esta página muestra si el puerto WAN está conectado a una conexión Cable/DSL. También muestra el puerto WAN del router: dirección IP WAN, Subnet Mask y ISP Gateway y también el Primary DNS y el Secondary DNS que se está utilizando.

4.3.4 Registro del sistema

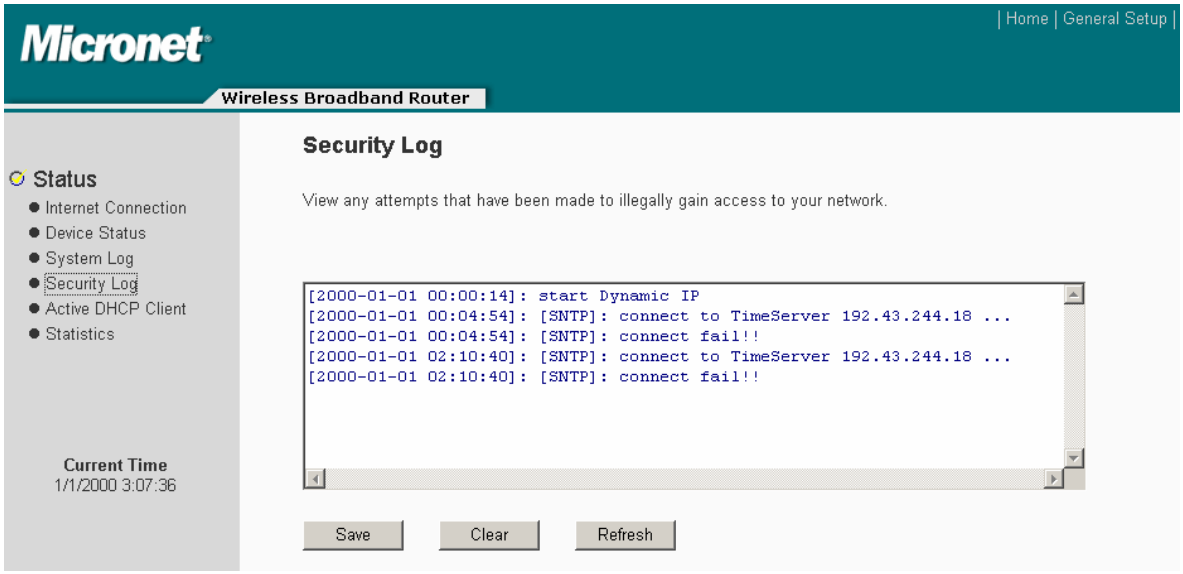
Vea el registro de operaciones del sistema. Todos los eventos importantes del sistema están registrados y los usuarios pueden utilizar esta función para revisar el registro de eventos del router.


Micronet
| Home | General Setup |
Wireless Broadband Router
Status
Internet Connection
Device Status
System Log
Security Log
Active DHCP Client
Statistics
Current Time
1/1/2000 3:06:42
System Log
View the system operation information. You can see the system start up time, connection process...etc. here.
Jan 1 00:00:00 (none) syslog.info syslogd started: BusyBox v1.00-pre2 (200
Jan 1 00:00:10 (none) local0.info udhcpd[396]: udhcpd (v0.9.9-pre) started
Jan 1 00:00:10 (none) local0.err udhcpd[396]: max_leases value (254) not s
Jan 1 00:00:15 (none) user.info udhcpc: udhcp client (v0.9.9-pre) started
Jan 1 00:03:06 (none) local0.info udhcpd[398]: sending OFFER of 192.168.2.
Jan 1 00:03:06 (none) local0.info udhcpd[398]: sending OFFER of 192.168.2.
Jan 1 00:03:09 (none) local0.info udhcpd[398]: sending ACK to 192.168.2.10
Jan 1 00:08:39 (none) local0.info udhcpd[398]: sending OFFER of 192.168.2.
Jan 1 00:08:44 (none) local0.info udhcpd[398]: sending OFFER of 192.168.2.
Save
Clear
Refresh

Parámetro	Descripción
System Log	Esta página muestra el registro del sistema actual del Broadband router. Muestra cualquier evento ocurrido después del inicio del sistema. En la parte inferior de la pantalla, el registro del sistema se puede guardar con el botón <**Save**> en un archivo local para continuar con el procesamiento. El registro del sistema se puede borrar haciendo clic en el botón <**Clear**>. Actualice la interfaz para ver la situación presente, haciendo clic en el botón <**Refresh**>. Cuando apague el sistema, el registro desaparecerá si no se guarda en un archivo local.

4.3.5 Registro de seguridad

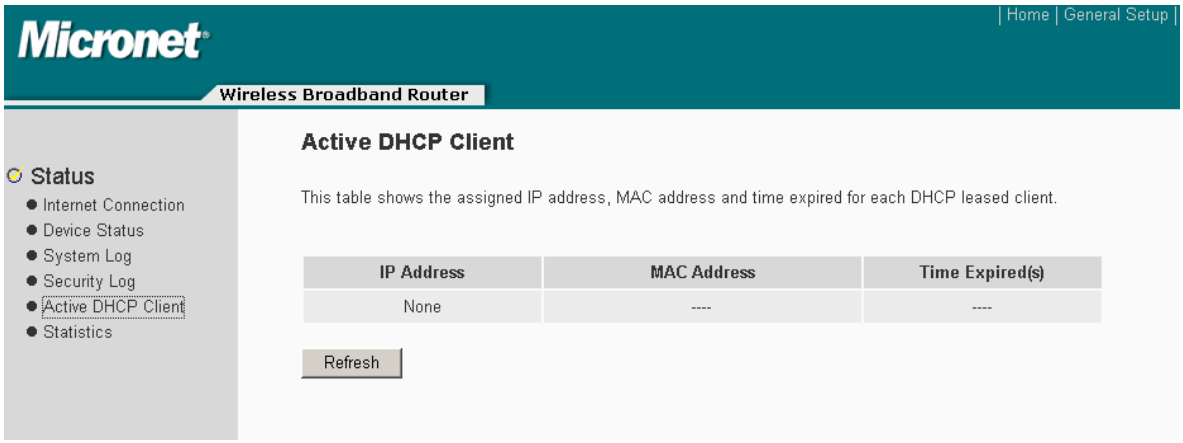
Vea cualquier intento que se haya hecho de obtener acceso ilegal a la red. Toda la información acerca de la red y el sistema de seguridad se guarda aquí y los usuarios pueden utilizar esta función para revisar el registro de eventos de seguridad del router.



Parámetro	Descripción
System Log	Esta página muestra el registro de seguridad actual del Broadband router. Muestra cualquier intento ilegal de acceder a la red. En la parte inferior de la pantalla, el registro de seguridad se puede guardar con el botón <**Save**> en un archivo local para continuar con el procesamiento. El registro de seguridad se puede borrar haciendo clic en el botón <**Clear**>. Actualice la interfaz para ver la situación presente, haciendo clic en el botón <**Refresh**>. Cuando apague el sistema, el registro de seguridad desaparecerá si no se guarda en un archivo local.

4.3.6 Cliente DHCP activo

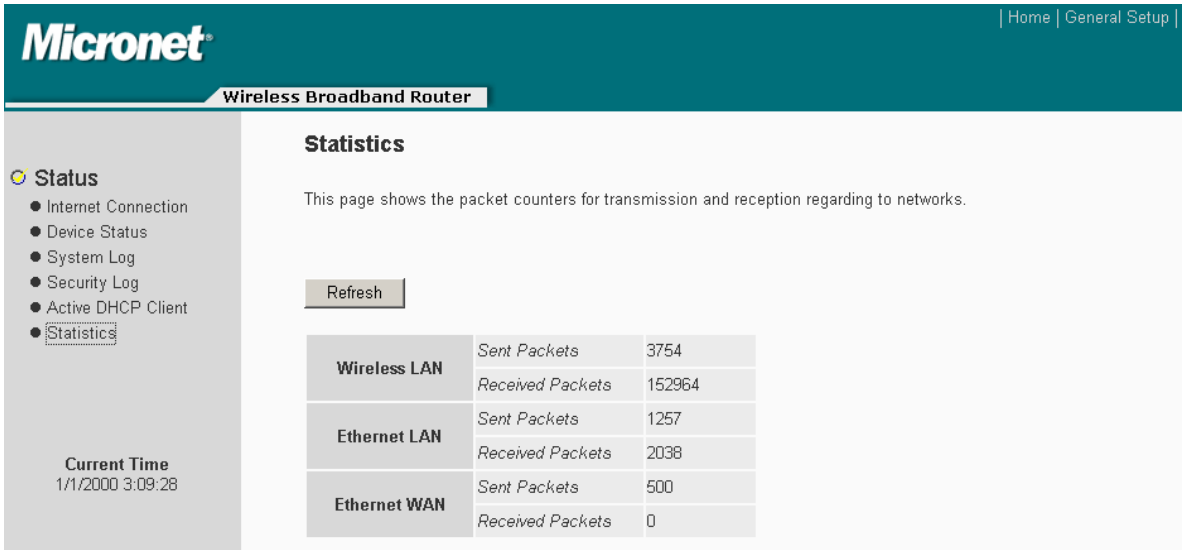
Vea la información del cliente LAN que está actualmente relacionada con el servidor DHCP del Broadband router.



Parámetro	Descripción
Active DHCP Client	Esta página muestra todos los clientes DHCP (LAN PCs) que están actualmente conectados a la red. La “Active DHCP Client Table” presenta la dirección IP, la dirección MAC y el Time Expired de cada cliente LAN. Utilice el botón <**Refresh**> para obtener la situación más actualizada.

4.3.7 Estadísticas

Vea las estadísticas de los paquetes enviados y recibidos en WAN, LAN y LAN inalámbrica.



Parámetro	Descripción
Statistics	Muestra el contador de paquetes enviados y recibidos en WAN, LAN y LAN inalámbrica.

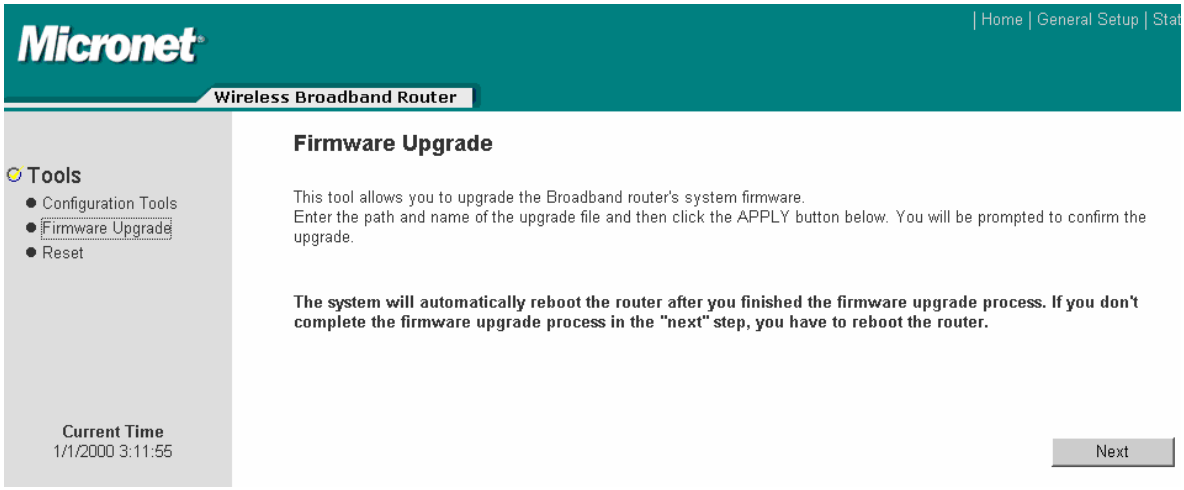
4.4 Configuración de respaldo y restauración

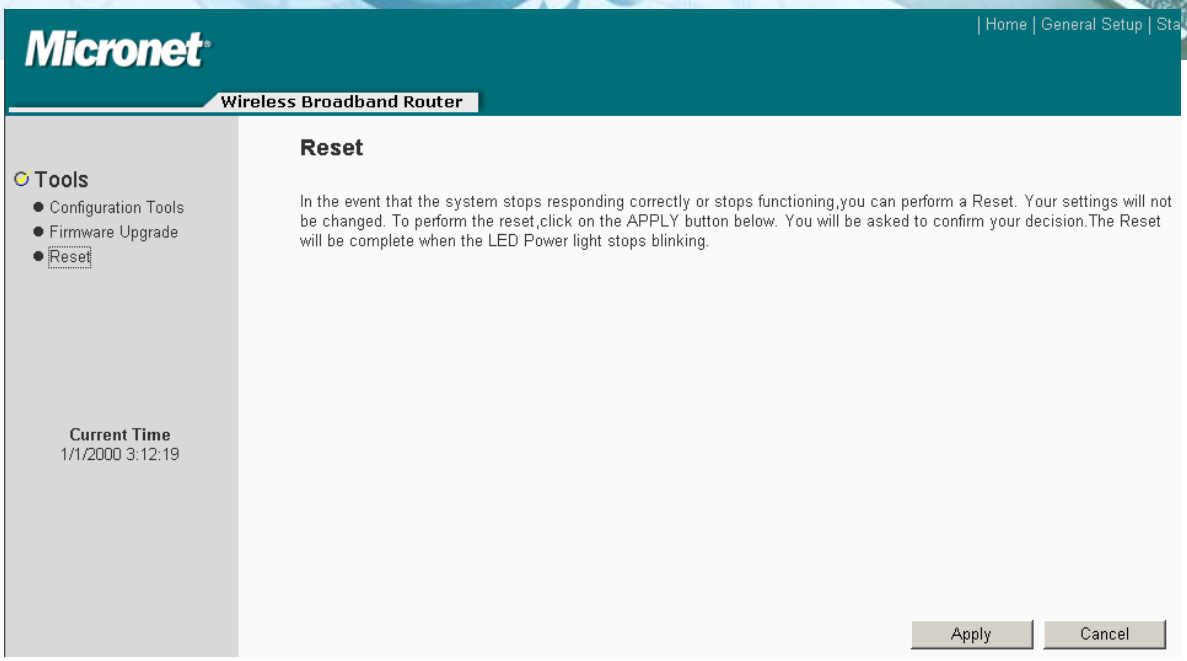
Esta página incluye las herramientas básicas de configuración, tales como Configuration Tools (guarda o restaura los ajustes de configuración), Firmware Upgrade (actualiza el firmware del sistema) y Reset.

Parámetro	Descripción
Configuration Tools	Utilice la herramienta “Backup” para guardar la configuración actual del Broadband router en un archivo llamado “config.bin” en la PC. Los usuarios pueden utilizar la herramienta “Restore” para restaurar la configuración guardada en el Broadband router. Asimismo, los usuarios pueden utilizar la herramienta “Restore to Factory Defaults” para forzar al Broadband router a ejecutar un reajuste y restaurar las configuraciones originales de fábrica.

4.5 Actualización de Firmware

El software de sistema utilizado por este router se llama “firmware”. Tal como cualquiera de las aplicaciones de la computadora, cuando los usuarios reemplazan la aplicación vieja por una nueva, la computadora se equipará con una nueva función. Los usuarios también pueden utilizar esta función de actualización de firmware para agregar nuevas funciones al router.


Micronet
| Home | General Setup | Stat
Wireless Broadband Router
Tools
Configuration Tools
Firmware Upgrade
Reset
Current Time
1/1/2000 3:11:55
Firmware Upgrade
This tool allows you to upgrade the Broadband router's system firmware.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.
The system will automatically reboot the router after you finished the firmware upgrade process. If you don't complete the firmware upgrade process in the "next" step, you have to reboot the router.
Next


Micronet
| Home | General Setup | Sta
Wireless Broadband Router
Tools
Configuration Tools
Firmware Upgrade
Reset
Current Time
1/1/2000 3:12:19
Reset
In the event that the system stops responding correctly or stops functioning,you can perform a Reset. Your settings will not be changed. To perform the reset,click on the APPLY button below. You will be asked to confirm your decision.The Reset will be complete when the LED Power light stops blinking.
Apply
Cancel

Parámetro	Descripción
Firmware Upgrade	Esta herramienta les permite a los usuarios actualizar el firmware del sistema del Broadband router. Para actualizar el firmware del router, los usuarios tienen que descargar el archivo de firmware al disco rígido local. Ingrese el nombre del archivo y la ruta en el campo apropiado en esta página. Como alternativa, puede utilizar el botón <**Browse**> para encontrar el archivo de firmware.

*Haga clic en el botón **<Apply>** en la parte inferior de la pantalla para guardar la configuración anterior.*

4.6 Reinicio del sistema

Los usuarios pueden reiniciar el sistema del router, si hubiese algún problema. La función de reinicio básicamente reinicia el sistema del router.

Parámetro	Descripción
Reset	En caso de que el sistema deje de responder correctamente o que, de alguna forma, deje de funcionar, los usuarios pueden ejecutar un reinicio. Las configuraciones no serán cambiadas. Para ejecutar el reinicio, haga clic en el botón <**Apply**>. Se les pedirá a los usuarios que confirmen su decisión. El reinicio estará completo cuando la luz de encendido deje de titilar. Una vez que el proceso de reinicio esté completo, los usuarios podrán utilizar

	el router nuevamente.